Headquarters:
No. 25, Alley 15, Lane 120,
Sec. 1. Nei-Hu Rd,
Taipei 114, Taiwan
TEL: 886-2-26583000
FAX: 886-2-26583232

Beijing Branch:
3F, A Building,
113 Zhi Chun Lu,
HaiDian District,
Beijing, China
Zip Code: 100086
TEL: 86-10-62522081~87
FAX: 86-10-62522077

USER'S MANUAL

Hi-Performance Network Security Solution

NetSecure 6100

Version: 1.0
Date: 2007/1/10
P/N: 0700800097

Copyright © 2007 TAINET Communication System Corp.
All rights reserved

Notice

This document is protected by the international copyright law. No part of this publication may be reproduced by any means without the expressed permission of Tainet Communication System Corporation.

TAINET is a registered trademark, and NetSecure 6100 is a trademark of Tainet Communication System Corporation.

Other product names mentioned in this manual are used for identification purposes only and may be trademarks or trademarks of their respective companies.

The information provided from Tainet Communication System Corporation is believed to be accurate. Any changes and enhancements to the product and to the information thereof will be documented and issued as a new release to this manual.

Trademark

All products and services mentioned herein are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.

About This Manual

This section guides users on how to use the manual effectively. The manual contains information needed to install, configure, and operate TAINET's NetSecure 6100. The summary of this manual is as follows:

Chapter 1: Overview

Chapter 2: Getting Started

Chapter 3: Security Zones and Interfaces

Chapter 4: System Management

Chapter 5: Attack Detection and Prevention

Chapter 6: Logging

Chapter 7: Virtual Private Networks

Chapter 8: Routing

Chapter 9: Policy Configuration

Chapter 10: Address Translation

Chapter 11: High Availability

Chapter 12: PKI and X.509/Digital Certificates

Appendix A: Pre-defined Service

Appendix B: Glossary

Symbols Used in This Manual

3 types of symbols may be used throughout this manual. These symbols are used to advise the users when a special condition arises, such as a safety or operational hazard, or to present extra information to the users. These symbols are explained below:

Warning:

This symbol and associated text are used when death or injury to the user may result if operating instructions are not followed properly.

Caution:

This symbol and associated text are used when damages to the equipment or impact to the operation may result if operating instructions are not followed properly.

Note:

This symbol and associated text are used to provide the users with extra information that may be helpful when following the main instructions in this manual.

LIMITED WARRANTY

TAINET's DISTRIBUTOR shall be responsible to its customers for any and all warranties, which it makes relating to Products, and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory. TAINET warrants to DISTRIBUTOR that the Products to be delivered hereunder will be free of defects in material and workmanship under normal use and service for a period of twenty-four (24) months [twelve (12) months in Taiwan] following the date of shipment to DISTRIBUTOR.

If during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and DISTRIBUTOR notifies TAINET of such defect within seven days after knowing of such defect, TAINET shall, for any Product that TAINET agrees is defective, at its option, supply a replacement part, request return of equipment to its plant for repair, or perform necessary repair at the equipment's location. At TAINET's option, DISTRIBUTOR shall destroy any Product that TAINET agrees is defective and shall provide satisfactory proof of such destruction to TAINET. TAINET is not responsible for Products damaged by misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than TAINET's own authorized service personnel, unless such repairs by others were made with the written consent of TAINET.

THE ABOVE WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED. THERE ARE NO WARRANTIES THAT EXTEND BEYOND THE FACE HEREOF, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND IN NO EVENT SHALL TAINET BE LIABLE FOR CONSEQUENTIAL DAMAGES. If DISTRIBUTOR extends to its customers any additional warranty with respect to Products that is broader in scope than the warranty provided by TAINET, DISTRIBUTOR shall be solely responsible for any and all liabilities, obligations and damages resulting from the extension of such warranty.

TAINET shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits, from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the Products, and in no event shall TAINET's liability exceed the purchase price of the Products.

Software Products are provided "as is" and without warranty of any kind. TAINET disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. TAINET shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. TAINET shall do its best to provide end users with Software updates during the warranty period under this Agreement.

TAINET has not been notified of any intellectual property rights or others which may be infringed by the Products or the promotion, marketing, sale (or resale), or servicing thereof in the Territory, but TAINET makes NO WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT THERETO.

CONTENTS

CHAPTER 1. OVERVIEW 1

1.1 ABOUT DOCUMENT CONVENTIONS 1
1.1.1 COMMAND LINE INTERFACE (CLI) CONVENTIONS 2
1.1.2 BROWSER-BASED GRAPHICAL USER INTERFACE (WEBGUI) CONVENTIONS 3
1.1.3 ILLUSTRATION CONVENTIONS 4

CHAPTER 2. GETTING STARTED 5

2.1 BEFORE YOU INSTALL 5
2.1.1 INSTALLATION PRECAUTIONS 5
2.1.2 WHAT YOU MUST KNOW FOR INSTALLATION 6
2.2 INSTALLING THE <NETSECURE 6100> 7
2.2.1 CONNECTING THE POWER 7
2.2.2 CONNECTING THE < NetSecure 6100> TO OTHER NETWORK DEVICES 7
2.2.3 CONFIGURING THE <NetSeure 6100> 8
2.2.4 CONNECTING THE CONSOLE CABLE 9
2.2.5 CONFIGURING THE SOFTWARE 9
2.2.6 CHANGING THE ADMIN PASSWORD 10
2.2.7 CONFIGURING INTERFACES 10
2.2.8 CONFIGURING NETWORK ADDRESS TRANSLATION (NAT) 12
2.2.9 CONFIGURING THE DEFAULT ROUTE 13
2.2.10 CONFIGURING A POLICY FROM TRUST TO UNTRUST 13
2.2.11 VIEWING THE POLICY CONFIGURATION 14

CHAPTER 3. SECURITY ZONE AND INTERFACES 15

3.1 SECURITY ZONES 15
3.2 CREATING AND MODIFYING CUSTOM SECURITY ZONES 18
3.2.1 CREATING CUSTOM SECURITY ZONES 18
3.2.2 DELETING CUSTOM SECURITY ZONES 18
3.2.3 BLOCKING WITHIN A ZONE 20
3.2.4 VIEWING ZONE CONFIGURATIONS 21
3.3 CONFIGURING INTERFACES AND SUBINTERFACES 23
3.3.1 CONFIGURING INTERFACES 23
3.3.2 BINDING INTERFACES TO A SECURITY ZONE 24
3.3.3 MOVING INTERFACES BETWEEN SECURITY ZONES 25
3.3.4 CONFIGURING SUBINTERFACES 25
3.3.5 DELETING SUBINTERFACES 26

3.4 CONFIGURING INTERFACE MODES 28
3.4.1 CONFIGURING NAT-ENABLED MODE 28
3.4.2 CONFIGURING ROUTE MODE 29
3.4.3 VIEWING INTERFACE INFORMATION 31
3.4.4 CONFIGURING TRANSPARENT MODE 32
3.5 ADVANCED INTERFACE SETTINGS 41
3.5.1 CONFIGURING MAXIMUM TRANSMISSION UNIT (MTU) SETTINGS 41
3.5.2 CONFIGURING INTERFACE LINK UP/DOWN 42
3.5.3 CONFIGURING ADDRESS RESOLUTION PROTOCOL (ARP) 42
3.6 AUTHENTICATION USING RADIUS 46
3.6.1 HOW THE RADIUS CHALLENGE-RESPONSE MODE WORKS 46
3.6.2 RADIUS CLIENT ATTRIBUTES 47
3.6.3 RADIUS BACKUP SERVER 50
3.7 ALTERNATE CONNECTION METHODS 54
3.7.1 PPPoE: POINT -TO-POINT PROTOCOL OVER ETHERNET 54
3.7.2 SETTING UP PPPoE 54

CHAPTER 4. SYSTEM MANAGEMENT 57

4.1 USING THE CONSOLE TO MANAGE THE <NETSECURE 6100> 57
4.1.1 ABOUT CONSOLE CABLE REQUIREMENTS 58
4.1.2 ACCESSING THE CONSOLE 59
4.1.3 RE-ENABLING THE CONSOLE INTERFACE 60
4.1.4 VIEWING CONSOLE INTERFACE SETTINGS 60
4.1.5 SETTING THE CONSOLE DISPLAY 60
4.1.6 SETTING THE CONSOLE TIMEOUT 60
4.1.7 EXITING THE CONSOLE 61
4.2 USING SSH TO MANAGE THE <NETSECURE 6100> 62
4.2.1 GENERATING SSH HOST KEYS 62
4.2.2 ENABLE SSH GLOBALLY 62
4.2.3 ENABLING SSH ON A SPECIFIC INTERFACE 62
4.2.4 DISABLING SSH ON A SPECIFIC INTERFACE 63
4.2.5 VIEWING SSH SETTINGS 63
4.3 MANAGING USERS FOR THE < NETSECURE 6100> 64
4.3.1 CHANGING YOUR ADMINISTRATOR PASSWORD 64
4.3.2 ABOUT ADDITIONAL TYPES OF USERS 65
4.3.3 CHANGING THE ADMIN-R PASSWORD 65
4.3.4 VIEWING CURRENT USERS 65
4.4 MANAGING SOFTWARE FOR THE < NETSECURE 6100> 66
4.4.1 STORING SOFTWARE IMAGE FILES IN FLASH MEMORY 66

4.4.2 DOWNLOADING NEW SOFTWARE 66
4.4.3 UPLOADING NEW SOFTWARE 66
4.4.4 SAVING MOS SOFTWARE TO FLASH MEMORY USING TFTP 67
4.4.5 SAVING BOOT SOFTWARE TO FLASH MEMORY USING TFTP 68
4.4.6 SETTING THE SOFTWARE AS PRIMARY OR SECONDARY 68
4.4.7 SAVING THE CONFIGURATION FILE FOR EXPORT 68
4.4.8 VIEW THE RUNNING CONFIGURATION 69
4.4.9 VIEW THE SAVED CONFIGURATION 69
4.5 RESETTING AND RESTARTING THE < NETSECURE 6100> 70
4.5.1 RESETTING THE APPLIANCE 70
4.5.2 RESETTING THE SOFTWARE 70
4.5.3 RESTARTING THE < NetSecure 6100> 71
4.6 ADDITIONAL SYSTEM MANAGEMENT TASKS 72
4.6.1 VIEWING SYSTEM INFORMATION 72
4.6.2 CREATING ALIASES 74
4.6.3 DELETING ALIASES 74
4.6.4 VIEWING CURRENT ALIASES 75
4.6.5 CONFIGURING DOMAIN NAMES 75
4.6.6 DELETING DOMAIN NAMES 75
4.6.7 CONFIGURING HOST NAMES 76
4.6.8 DELETING HOST NAMES 76
4.7 USING NETWORK TIME PROTOCOL (NTP) 77
4.7.1 CONFIGURING NTP SETTINGS 77
4.7.2 CONFIGURING THE NTP UPDATE INTERVAL 78
4.7.3 VIEWING CURRENT NTP SETTINGS 78
4.7.4 DELETING NTP SERVER IP ENTRIES 78
4.7.5 CONFIGURING MANUAL UPDATE USING NTP 79
4.7.6 MAINTAINING CLOCK SETTINGS WITH NTP 79
4.7.7 CONFIGURING THE CLOCK TO USE NTP 80
4.7.8 CONFIGURING THE TIME ZONE 80
4.8 USING DOMAIN NAME SERVICE (DNS) 81
4.8.1 DELETING DNS HOST IP ADDRESSES 82
4.8.2 DISPLAYING CURRENT DNS HOST SETTINGS 82
4.9 USING PING 83
4.10 USING TRACEROUTE 84

CHAPTER 5. ATTACK DETECTION & PREVENTION 85

5.1 NETWORK ATTACKS 85
5.2 ATTACK STAGES 87

5.3 DETECTING AN ATTACK 88
5.4 ABOUT DENIAL OF SERVICE (DOS AND DDOS) ATTACKS 90
5.5 PREVENTING NETWORK PORT ATTACKS 92
5.6 CONFIGURING THE < NETSECURE 6100> TO DEFEND AGAINST DOS AND DDOS ATTACKS 94
5.6.1 CONFIGURING ICMP FLOOD PREVENTION 94
5.6.2 CONFIGURING UDP FLOOD PREVENTION 95
5.6.3 CONFIGURING SYN FLOOD PREVENTION 95
5.6.4 CONFIGURING FIN FLOOD PREVENTION 96
5.6.5 CONFIGURING IP FRAGMENT PREVENTION 97
5.6.6 CONFIGURING TCP-FIN-NO-ACK 97
5.7 ADDITIONAL ATTACK DETECTION AND PREVENTION 99
5.8 VIEWING ATTACK SETTINGS 100

CHAPTER 6. LOGGING 101

6.1 LOGGING 101
6.2 LOGGING LEVELS 102
6.3 LOG MODULES 103
6.4 TRAFFIC AND EVENT LOG MANAGEMENT 104
6.5 LOG MODULE SETTINGS 105
6.5.1 SETTING LOG MODULES 105
6.5.2 DISABLING LOG MODULE SETTINGS 105
6.5.3 VIEWING THE LOG MODULE SETTINGS 106
6.5.4 VIEWING THE TRAFFIC AND EVENT LOG 107
6.6 ADMIN MAIL SERVER 108
6.6.1 CONFIGURE THE SECURITY APPLIANCE TO SEND E-MAIL NOTIFICATION USING THE ADMIN MAIL OPTION 108
6.6.2 DELETING THE ADMIN MAIL SERVER 109
6.6.3 REMOVING E-MAIL ADDRESSES FROM THE ADMIN MAIL SERVER 109
6.7 SYSLOG MANAGEMENT 110
6.7.1 DELETING THE SYSLOG HOST IP ADDRESS 111
6.7.2 DISABLING THE SYSLOG HOST LOG OPTIONS 111
6.7.3 SYSLOG MESSAGE FORMAT 111
6.7.4 SYSLOG MESSAGE SAMPLE: 111
6.8 SNMP MIB GROUPS 113
6.8.1 SYSTEM GROUP 113
6.8.2 INTERFACE GROUP 114
6.8.3 ADDRESS TRANSLATION GROUP 114
6.8.4 IP GROUP 114

6.8.5 IP ADDRESS 115
6.8.6 IP ROUTE 116
6.8.7 IP NET TO MEDIA 116
6.8.8 ICMP GROUP SCALARS 117
6.8.9 TCP GROUP SCALARS 118
6.8.10 TCP CONNECTION 118
6.8.11 UDP GROUP SCALARS 119
6.8.12 UDP LISTENER 119
6.8.13 SNMP GROUP 119
6.8.14 TRANSMISSION GROUP (DOT3STATS) 120
6.8.15 TRANSMISSION GROUP (DOT3COLLISION) 121
6.9 CONFIGURING SNMP ON THE SECURITY APPLIANCE 122
6.9.1 ENABLING SNMP ON A SPECIFIED INTERFACE 122
6.9.2 CONFIGURING THE SNMP COMMUNITY STRING 123
6.9.3 CONFIGURING THE SNMP LISTENER PORT 123
6.9.4 CONFIGURING THE SNMP SYSTEM NAME 124
6.9.5 DELETING THE SNMP SYSTEM NAME 124
6.9.6 CONFIGURING THE SNMP SYSTEM LOCATIONS 124
6.9.7 DELETING THE SNMP LOCATION 124
6.9.8 CONFIGURING THE SNMP SYSTEM CONTACT 124
6.9.9 DELETING THE SNMP SYSTEM CONTACT 125
6.9.10 VIEWING THE SNMP SETTINGS 125
6.9.11 VIEW THE SNMP COMMUNITY SETTINGS 125
6.9.12 VIEW THE SNMP STATISTICS 125
6.9.13 VIEWING THE INTERFACE STATISTICS 127

CHAPTER 7. VIRTUAL PRIVATE NETWORKS 129

7.1 VIRTUAL PRIVATE NETWORKS 129
7.1.1 ABOUT IP SECURITY (IPSEC) 130
7.1.2 TRANSPORT MODE 130
7.1.3 TUNNEL MODE 131
7.1.4 THE DIFFIE-HELLMAN GROUP 132
7.1.5 SECURITY ASSOCIATION 133
7.1.6 SITE-TO-SITE VPN REQUIREMENTS 133
7.1.7 VPN SPECIAL CONSIDERATIONS 134
7.2 CONFIGURING MANUAL KEY VPN IMPLEMENTATIONS 135
7.2.1 CREATING MANUAL KEY VPN TUNNELS 135
7.2.2 CREATING SECURITY POLICY WITH THE VPN TUNNELS 136
7.2.3 DELETING MANUAL KEY VPN TUNNELS 144

7.2.4 MODIFYING MANUAL KEY VPN TUNNELS 144
7.3 CONFIGURING INTERNET KEY EXCHANGE 145
7.3.1 CREATING IKE PHASE 1 AND PHASE 2 PROPOSALS 145
7.3.2 CONFIGURING AN IKE TUNNEL USING A PRE-SHARED SECRET 147
7.3.3 TRANSPARENT MODE VPN DEPLOYMENT 155
7.3.4 CONFIGURATION OF VF A 156
7.3.5 CONFIGURATION OF VF B 157
7.4 ADVANCED VPN CONFIGURATION OPTIONS 158
7.4.1 DEAD PEER DETECTION (DPD) 158
7.4.2 NAT-TRAVERSAL (NAT-T) 159
7.4.3 PERFECT FORWARD SECRECY (PFS) 159
7.4.4 REPLAY PROTECTION 160
7.4.5 VIEW A VPN TUNNEL 160
7.4.6 VIEW IKE INFORMATION 160
7.4.7 VIEW IKE GATEWAY 161
7.4.8 VIEW IKE PHASE 1 PROPOSALS 161
7.4.9 VIEW IKE PHASE 2 PROPOSALS 161

CHAPTER 8. ROUTING 163

8.1 STATIC ROUTES 163
8.1.1 ADDING STATIC ROUTES 164
8.1.2 DELETING STATIC ROUTES 165
8.1.3 MODIFYING STATIC ROUTES 165
8.2 SETTING THE DEFAULT ROUTE 166
8.3 DISPLAYING ROUTE INFORMATION 167
8.4 ROUTING INFORMATION PROTOCOL (RIP) 169
8.5 CONFIGURING RIP 170
8.6 ENABLING AND DISABLING RIP ON INTERFACES 171
8.7 DISABLE ROUTE SUMMARIZATION 172
8.8 ENABLE OR DISABLE SPLIT HORIZON 173
8.9 ENABLE RIP AUTHENTICATION 174
8.10 ACCEPTING PACKETS WITH NON -ZERO RESERVED FIELDS 175

CHAPTER 9. POLICY CONFIGURATION 177

9.1 ABOUT SECURITY POLICIES 177
9.1.1 ABOUT TRAFFIC FLOW AMONG POLICIES 177
9.1.2 ABOUT SECURITY POLICY TYPES 178
9.2 CONFIGURING POLICIES 181
9.2.1 CREATING POLICIES 181

9.2.2 NAMING POLICIES 183
9.2.3 REORDERING POLICES 184
9.2.4 DISABLING POLICIES 185
9.2.5 RE-ENABLING POLICIES 185
9.2.6 DELETING POLICIES 185
9.2.7 VIEWING POLICIES 185
9.2.8 ENABLE POLICY LOGGING 188
9.3 CONFIGURING ADDRESS OBJECTS 189
9.3.1 CREATING ADDRESS OBJECTS 189
9.3.2 DELETING ADDRESS OBJECTS 191
9.3.3 MODIFYING ADDRESS OBJECTS 191
9.3.4 CREATING ADDRESS GROUPS 192
9.3.5 DDING OBJECTS TO AN ADDRESS GROUP 193
9.3.6 DELETING ADDRESS GROUPS 194
9.3.7 DELETING ADDRESS OBJECTS FROM AN ADDRESS GROUP 195
9.3.8 ADDING COMMENTS TO ADDRESS GROUPS 195
9.4 CONFIGURING SERVICE OBJECTS 196
9.4.1 VIEWING PREDEFINED SERVICE OBJECTS 196
9.4.2 CONFIGURING CUSTOM SERVICE OBJECTS 196
9.4.3 DELETING SERVICE OBJECTS 197
9.4.4 MODIFYING SERVICE OBJECTS 197
9.4.5 CONFIGURING SERVICE TIMEOUTS 198
9.5 CONFIGURING SERVICE GROUPS 199
9.5.1 CREATING SERVICE GROUPS 199
9.5.2 DELETING SERVICE GROUPS 200
9.5.3 REMOVING SERVICE OBJECTS FROM GROUPS 201
9.5.4 MODIFYING SERVICE GROUPS 201
9.5.5 ADDING COMMENTS TO SERVICE GROUPS 202
9.6 ABOUT SCHEDULES 203
9.6.1 CREATING ONE -TIME SCHEDULES 203
9.6.2 CREATING RECURRING SCHEDULES 204
9.6.3 ADDING SCHEDULES TO POLICIES 205
9.6.4 DELETING SCHEDULES 206
9.6.5 VIEWING SCHEDULES 206

CHAPTER 10. ADDRESS TRANSLATION 209

10.1 NETWORK ADDRESS TRANSLATION 209
10.2 CONFIGURING SOURCE NETWORK ADDRESS TRANSLATION 211
10.2.1 ABOUT PORT ADDRESS TRANSLATION (PAT) 211

10.2.2 CONFIGURING DYNAMIC IP (DIP) POOLS 212
10.3 SOURCE NAT CONFIGURATIONS 213
10.3.1 CONFIGURING SOURCE NAT: MANY-TO-ONE WITH PORT ADDRESS TRANSLATION 213
10.3.2 CONFIGURING SOURCE NAT: MANY-TO-MANY WITH PORT ADDRESS TRANSLATION 213
10.4 CONFIGURING DESTINATION NAT AND PORT MAPPING 215
10.5 DESTINATION NAT CONFIGURATIONS 216
10.5.1 CONFIGURING DESTINATION NAT: ONE-TO-ONE 216
10.5.2 CONFIGURING DESTINATION NAT: ONE-TO-ONE WITH PORT MAPPING 217
10.5.3 CONFIGURING DESTINATION NAT: MANY-TO-ONE 217
10.5.4 CONFIGURING DESTINATION NAT: MANY-TO-ONE WITH PORT MAPPING 217
10.5.5 CONFIGURING DESTINATION NAT: MANY-TO-MANY 217

CHAPTER 11. HIGH AVAILABILITY 219

11.1 ABOUT HIGH AVAILABILITY 219
11.2 SOFTWARE ARCHITECTURE OVERVIEW 220
11.3 CLI COMMANDS 221
11.4 HA CONFIGURATION 222
11.4.1 CONFIGURING THE PRIMARY AND SECONDARY IP ADDRESSES FOR THE INTERFACE 222
11.4.2 CONFIGURING HA PRIORITY (VALUES 1 TO 254) 223

CHAPTER 12. PKI & X.509/DIGITAL CERTIFICATES 227

12.1 ABOUT PUBLIC KEY INFRASTRUCTURE AND X.509/DIGITAL CERTIFICATES .. 227
12.2 PKI BASICS 228
12.2.1 A TYPICAL DIGITAL CERTIFICATE 228
12.2.2 SELF-SIGNED CERTIFICATE 229
12.3 CLI COMMANDS 230
12.3.1 GENERATING A SELF-SIGNED CERTIFICATE 230
12.3.2 CREATING A CERTIFICATE REQUEST 231
12.3.3 IMPORTING A CERTIFICATE 232
12.3.4 USING A CERTIFICATE FOR A VPN TUNNEL 232

APPENDIX A PRE-DEFINED SERVICE 233

APPENDIX B GLOSSARY 235

FIGURES

Figure 1-1 shows the graphics used in illustrations in this guide. 4
Figure 2-1 Connecting the <NetSecure 6100> to other Network Device 8
Figure 2-2 Network Protection 11
Figure 3-1 Security Zone 16
Figure 3-2 Security Zones and Interfaces 16
Figure 3-3 Security Zone (Trust and Untrust)....17
Figure 3-4 Custom Security Zones 17
Figure 3-5 Get Zone Command Example 21
Figure 3-6 Eth0 and Eth1 Locations 23
Figure 3-7 NAT-Enabled Mode 29
Figure 3-8 Route Mode 30
Figure 3-9 Transparent Mode 34
Figure 3-10 Transparent Mode with VLAN Filtering 36
Figure 3-11 RADIUS Challenge Response Message Exchange....46
Figure 3-12 Configuring a Primary and Secondary RADIUS Server 51
Figure 5-1 Example of a DoS Attack 94
Figure 7-1 VPN Connectivity....130
Figure 7-2 VPNs Using Transport Mode 131
Figure 7-3 Using Tunnel Mode....131
Figure 7-4 Site-to-site VPN 133
Figure 7-5 Example of Manual Key VPN 137
Figure 7-6 IKE VPN Using a Pre-Shared Secret....146
Figure 7-7 VPN in Transparent Mode 155
Figure 8-1 Using a Static Route 164
Figure 8-2 Get Route Command Output 167
Figure 8-3 Get Route Command with ip_addr option Output 168
Figure 9-1 Display the use of security policies 178
Figure 9-2 Interzone Policy 179
Figure 9-3 Intrazone Policy 180
Figure 9-4 Address Objects 190
Figure 9-5 Address Groups 193
Figure 9-6 Service Groups 200
Figure 10-1 Source IP Address Translation 211
Figure 10-2 Source IP Address Translation with Port Address Translation 213
Figure 10-3 Destination NAT with Port Mapping 215
Figure 10-4 Destination Network Address Translation 216
Figure 10-5 Destination Network Address Translation with Address Shifting 218

Figure 11-1 High Availability Functionality Implemented through Custom Finite State Machines (FSM) 220
Figure 12-1 Digital Certificate Overview 228
Figure 12-2 Typical Digital Certificate 229

TABLES

Table 1-1 Variable CLI Values Used in This Guide....2
Table 2-1 Console Cable Pin-Out....8
Table 4-1 Console Cable Pin-out....58
Table 5-1 Network and Operating System –Specific Attacks....88
Table 5-2 DoS and DdoS Attacks....90
Table 6-1 Syslog Message Format....112
Table 6-2 System Group....113
Table 6-3 Interface Group....114
Table 6-4 Address Translation Group....114
Table 6-5 IP Group....114
Table 6-6 IP Address Table....115
Table 6-7 IP Route Table....116
Table 6-8 IP Net to Media Table....116
Table 6-9 ICMP Group Scalars....117
Table 6-10 ICMP Group Scalars....118
Table 6-11 TCP Connection Table....118
Table 6-12 UDP Scalars Table....119
Table 6-13 UDP Listener Table....119
Table 6-14 SNMP Group Table....119
Table 6-15Transmission Group (DOT3STATS Table)....120
Table 6-16 Transmission Group (DOT3COLLISION Table)....121
Table 7-1 MD5 and SHA-1 Description....132
Table 7-2 Required Manual Key VPN Parameters....135
Table 7-3 Policy Requirements for Manual Key VPN....136
Table 7-4 Example of Encryption and Authentication Settings....137
Table 7-5 Required Phase 1 and Phase 2 IKE Proposal Settings....145
Table 7-6 IKE Encryption and Authentication Settings....146
Table 9-1: Addresses and Zones....181
Table 9-2 One-time Schedule....204
Table 9-3 Recurring Schedule....204
Table A- 1 Pre-defined Service....233
Table A- 2 Protocols....234

Chapter 1. Overview

The NetSecure 6100 is a Gigabit security appliance that addresses the security requirements of today's high performance networks on the perimeter and interior LAN segments. Equipped with an extensive firewall feature set, the NetSecure 6100 has the capability to protect network hosts from wide ranging and high volume attacks meant to take network resources offline.

Features available on the <NetSecure 6100> include:

- Stateful packet inspection
- IPsec VPN
- Prevention of 30+ DoS and DDoS attacks
- Extensive Network Address Translation (NAT) features including: one-to-one, many-to-one, many-to-many, and port address translation (PAT)
- 802.1Q VLAN support
- Granular access control using network objects, services, and schedules
- Zone based security
- Secure CLI management using SSH

1.1 ABOUT DOCUMENT CONVENTIONS

This section explains the Command Line Interface (CLI), the browser based graphical user interface (WebGUI), and the illustration conventions used in this guide.

1.1.1 COMMAND LINE INTERFACE (CLI) CONVENTIONS

The following conventions are used when presenting the syntax of the command line interface (CLI):

- Values inside square brackets [ ] are optional.
- Values inside braces { } are required.
- For commands that require a selection from a pre-defined list of values, each value in the list is separated by a pipe (|).
- Variables appear in italic.
- When a CLI command appears within the context of a sentence in this document, it is in bold (except for variables, which are always in italic). For example: “Use the get system command to display general information about the <NetSecure 6100>.”

Variable CLI values are described in Table 1-1

Table 1-1 Variable CLI Values Used in This Guide

Variable CLI Value	Description
addr_str	Defines an IP address range assignment
dst_adr	Destination address assigned in a policy
fqdn	Fully Qualified Domain Name
ip_addr	Defines an IP address assignment
number	Numeric value assigned for a specific command
name_str	Name value assignment
password_str	New password assignment is required
src_adr	Source address assigned in a policy
srvc	Service assigned in a policy
zone name	Zone used in a specific command

1.1.2 BROWSER-BASED GRAPHICAL USER INTERFACE (WEBGUI) CONVENTIONS

- Values inside square brackets [ ] are optional.
- Values inside braces { } are required.
- For commands that require a selection from a pre-defined list of values, each value in the list is separated by a pipe (|).
- Variables appear in italic.

When a WebGUI command appears within the context of a sentence in this document, it is in **bold** (except for variables, which are always in *italic*). For example: “Use click on the **XXXX** command to display general information about the <NetSecure 6100>.”

1.1.3 ILLUSTRATION CONVENTIONS

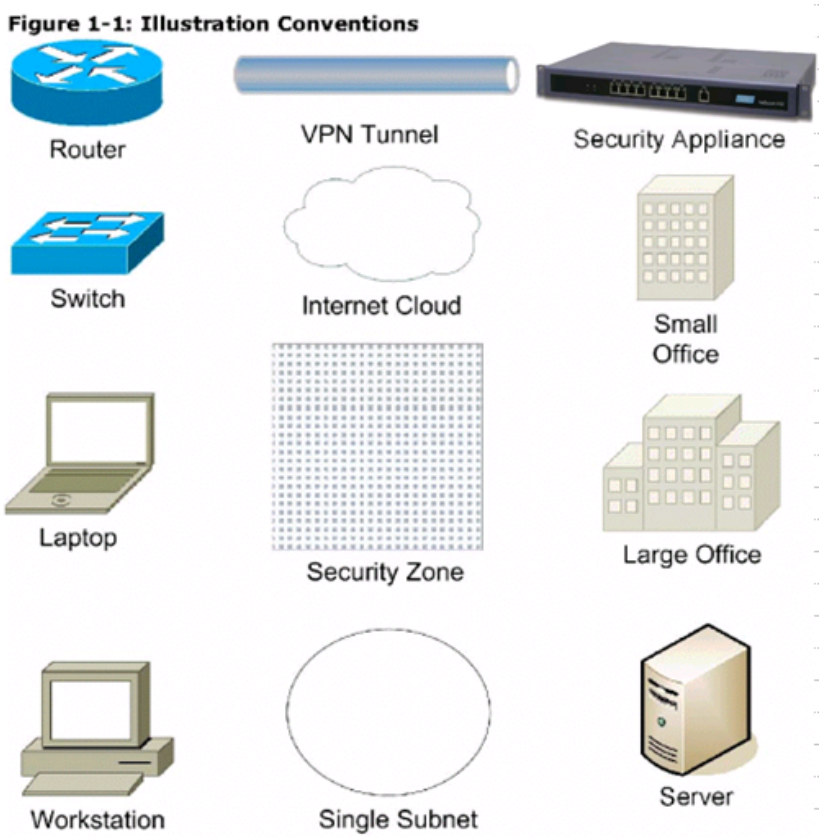


Figure 1-1 shows the graphics used in illustrations in this guide.

Chapter 2. Getting Started

This chapter describes how to install, configure, and manage the <NetSecure 6100>. This chapter includes the following topics:

- Before You Install
- Installing the <NetSecure 6100>

2.1 BEFORE YOU INSTALL

Familiarize yourself with the following topics before installing the <NetSecure 6100>:

- Before You Install
- Installing the <NetSecure 6100>

2.1.1 INSTALLATION PRECAUTIONS

Warning:

Obey these precautions when you install the <NetSecure 6100>. Observing these precautions can prevent injuries, equipment failures, and potential shutdown of the <NetSecure 6100>.

Warning:

Always assume the power supply for the <NetSecure 6100> is connected to the power outlet.

Caution:

Room temperature might not be adequate for long term use of the <NetSecure 6100>; for optimum environmental requirements for the <NetSecure 6100>, refer to the NetSecure 6100 Specifications Guide.

Caution:

Be careful of additional hazards, including frayed power cords, wet or moist floors, and missing safety grounds.

2.1.2 WHAT YOU MUST KNOW FOR INSTALLATION

You must understand the following concepts before you install the <NetSecure 6100> for the first time:

- Basic understanding of TCP/IP.
- IP addresses and subnet masks.
- Network Address Translation (NAT). For more information, refer to Chapter 10
- Creating a policy. For more information, refer to Chapter 9
- Routing. For more information, refer to Chapter 8
- Security zones. For more information, refer to Chapter 3

2.2 INSTALLING THE <NetSecure 6100>

This section guides you through the installation of the <NetSecure 6100>. Once you are familiar with the previous section, 2.1BEFORE YOU INSTALL prepare to proceed with the actual installation.

To install the <NetSecure 6100>, perform the tasks described in the following sections:

- Connecting the Power
- Connecting the <NetSecure 6100> to Other Network Devices
- Configuring the <NetSecure 6100>

2.2.1 CONNECTING THE POWER

You must connect a power source to the <NetSecure 6100> before you configure the appliance.

To connect the power:

- On the <NetSecure 6100>, plug the DC connector end of the power cable into the DC power receptacle on the back of the appliance.
- Plug the AC adapter end into a surge protected AC power source. The <NetSecure 6100> is now powered ON.

2.2.2 CONNECTING THE < NetSecure 6100> TO OTHER NETWORK DEVICES

Once the power is connected to the <NetSecure 6100>, you can connect it to other network devices. Use either of the two Ethernet interfaces labeled eth0 and eth1. Use these interfaces to connect other network devices as necessary.

Figure 2-1 displays the eth1 interface connected to an Internet router using a twisted pair Ethernet cable, while the eth0 interface is connected to a switch on

your local area network (LAN) using another twisted pair Ethernet cable.

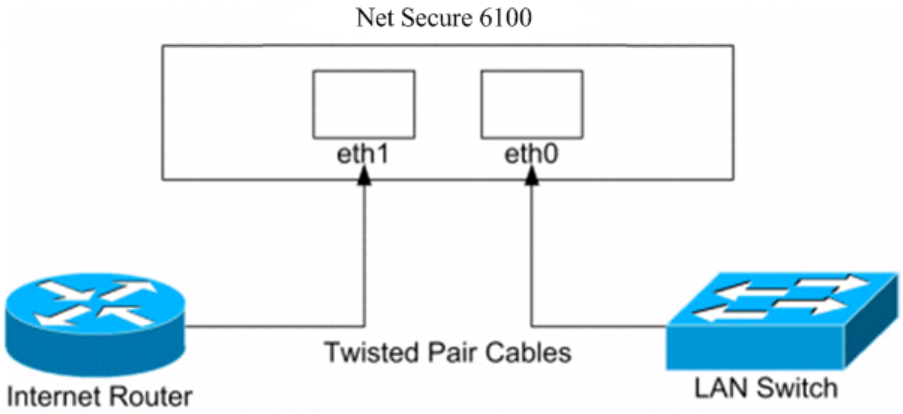


Figure 2-1 Connecting the <NetSecure 6100> to other Network Device

2.2.3 CONFIGURING THE <NetSeure 6100>

After you supply power to the <NetSecure 6100>, use the console interface to initially configure the card.

Table 2-1 lists the required console cable pin-out that you use to manage the <NetSecure 6100>.

Table 2-1 Console Cable Pin-Out

Female 2x5 Header	Female DB9
1	1
2	6
3	2
4	7
5	3
6	8
7	4
8	9
9	5
10	NC

2.2.4 CONNECTING THE CONSOLE CABLE

To use the console interface, you must connect the null modem cable included in the product packaging.

To connect the console cable to the <NetSecure 6100>:

- Connect the female 2x5 header of the console cable to the console port on the <NetSecure 6100>.
- Connect the other female DB9 connector to a serial interface on a laptop or desktop machine.
- To access the <NetSecure 6100> console interface, launch a terminal emulation program.

[NOTE] Hyper-Terminal by Hillgraeve Inc. is a suitable terminal emulation program, and is included with most Windows operating systems.

The default login credentials are *admin* and *admin*. These credentials are case sensitive.

- Enter the following settings in the terminal application:
  - Baud Rate—38,400
  - Parity—No
  - Data Bits—8
  - Stop Bit—1
  - Flow Control—None
- Press Enter to view the login prompt
- At the login prompt, type admin.
- At the password prompt, type admin.

2.2.5 CONFIGURING THE SOFTWARE

To configure the <NetSecure 6100> software for the first time, perform the steps

in the following sections:

- Changing the Admin Password
- Configuring Interfaces
- Configuring Network Address Translation (NAT))
- Configuring the Default Route
- Configuring a Policy from Trust to Untrust
- Viewing the Policy Configuration

2.2.6 CHANGING THE ADMIN PASSWORD

Because all <NetSecure 6100s> are preconfigured with the same password, you must change the admin password.

Use the **set admin** command to change the password:

- set admin password {password_str}
- save

2.2.7 CONFIGURING INTERFACES

Configure the <NetSecure 6100> to protect a network like that displayed in Figure 2-2. This configuration allows all workstations connected to the `eth0` interface to use the <NetSecure 6100> as their default gateway to the Internet. In this configuration, the `eth0` interface is connected to the inside LAN Switch and the `eth1` interface is connected to your Internet router. The `eth0` interface is bound to the zone `trust` and the `eth1` interface is bound to the zone `untrust`. This allows you to manage access control between the zones.

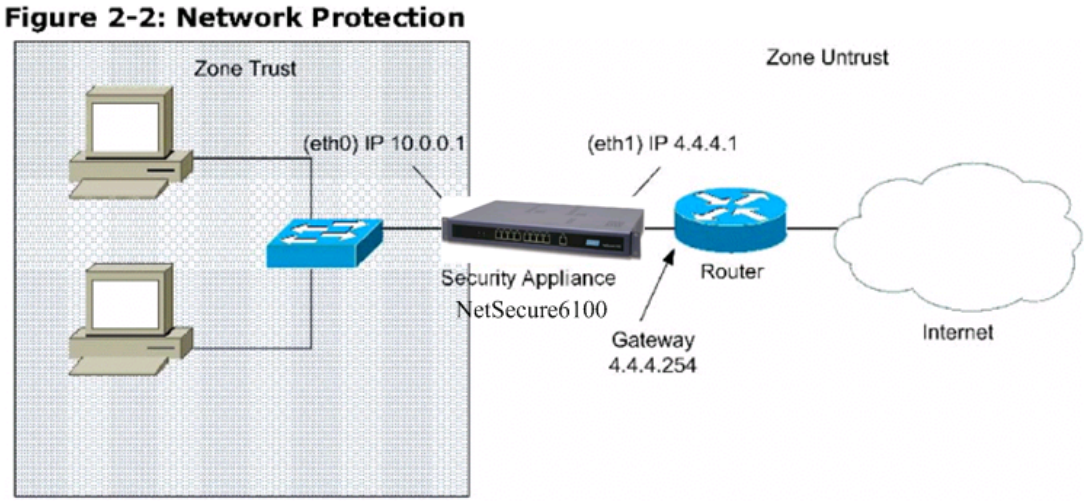


Figure 2-2 Network Protection

Use the **set interface** command to assign the zone, IP address and netmask to both interfaces as shown in Figure 2-2.

Example: Configuring Interface ETH0

Use the **set interface** command to bind the eth0 interface to the trust zone with an IP address and netmask of *10.0.0.1/24*:

- set interface eth0 ip 10.0.0.1/24
- set interface eth0 zone trust
- save

GUI Example: Configuring Interface ETH0

- Network > Interface > Edit (for eth0)
- Enter the following, then click **Apply**:
  - Zone Name: Trust
  - Static IP: (select this option when present)
  - IP Address/Netmask: 10.0.0.1/24

Example: Configuring Interface ETH1

Use the **set interface** command to bind the eth1 interface to the trust zone with an IP address and netmask of *4.4.4.1/24*:

- set interface eth1 ip 4.4.4.1
- set interface eth1 zone untrust
- save

Optional—To verify the new interface settings, use the **get interface** command:

- get interface {eth0|eth1}

GUI Example: Configuring Interface ETH1

1. Network > Interface > Edit (for eth1)
2. Enter the following, then click **Apply**:
   - Zone Name: Untrust
   - Static IP: (select this option when present)
   - IP Address/Netmask: 10.0.0.1/24

2.2.8 CONFIGURING NETWORK ADDRESS TRANSLATION (NAT)

To configure the <NetSecure 6100> to support a large number of hosts on the eth0 interface behind a single public IP address assigned to the eth1 interface, you must configure network address translation (NAT). For additional information regarding NAT configurations, refer to Chapter 10 Address Translation

Use the **set interface** command to apply NAT to all packets as they pass through the eth0 interface:

- set interface eth0 nat
- save

Optional—To verify the new interface settings, execute the get interface

command:

- get interface eth0

2.2.9 CONFIGURING THE DEFAULT ROUTE

Use the **set route** command to configure the default route for all traffic. The **set route** command consists of the destination network, the interface name, and the IP address to forward packets from that interface.

Using the network in Figure 2-2 as an example, use the **set route** command to configure the <NetSecure 6100> to use the eth1 interface and a gateway address of 4.4.4.254 for the default route of all traffic

- set route 0.0.0.0/0 interface eth1 gateway 4.4.4.254
- save

Optional: to verify the default route settings execute the **get route summary** command:

- get route summary

2.2.10 CONFIGURING A POLICY FROM TRUST TO UNTRUST

The default policy behavior is to not allow traffic to or from any zone that does not match a policy. In the example in Figure 2-2, you must create a policy allowing any traffic from the trust to the untrust zone. This is a common policy to enable hosts on the LAN connected to the trust zone to browse the Internet using a web browser.

Use the **set policy** command to create a policy allowing any traffic going from the trust zone to the untrust zone:

- set policy from trust to untrust any any any permit
- save

[NOTE] For more information about configuring policies, refer to Chapter 9 Policy

Configuration

2.2.11 VIEWING THE POLICY CONFIGURATION

Use the get config command to view the policy configuration:

- get config

This command returns the following information, which is based on the network diagram in Figure 2-2:

Interfaces

- set interface eth0 ip 10.0.0.1/24
- set interface eth0 zone trust
- set interface eth0 nat
- set interface eth1 ip 4.4.4.1/24
- set interface eth1 untrust

Route

- set route 0.0.0.0/0 interface eth1 gateway 4.4.4.254

Policy

- set policy from trust to untrust any any any permit

Chapter 3. Security Zone and Interfaces

This chapter describes how to configure zones, interfaces, modes of operation and advanced interface settings for the security appliance. This chapter includes the following topics:

- Security Zones
- Creating and Modifying Custom Security Zones
- Configuring Interfaces and Subinterfaces
- Configuring Interface Modes
- Advanced Interface Settings
- Authentication Using RADIUS
- Alternate Connection Methods

3.1 SECURITY ZONES

Security zones are a logical grouping of physical and logical interfaces on an appliance. A security zone can consist of one physical interface or a group of many physical and logical interfaces. Security policies incorporate security zones to efficiently manage access control policies of traffic that traverses zones and interfaces.

Figure 3-1 displays the interface eth0 configured in the trust zone with two subinterfaces: VLAN 100 and 105. Two additional subinterfaces are added in the DMZ zone: VLAN 200 and 210. The eth1 interface is configured in the untrust zone.

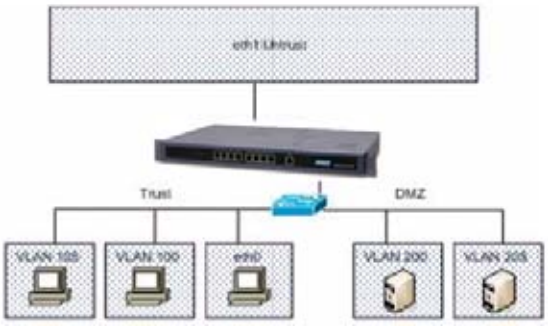
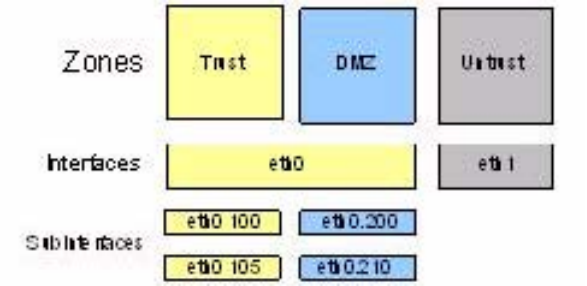


Figure 3-1 Security Zone

Figure 3-2shows the interface eth0 being configured in the trust zone along with two additional subinterfaces, VLAN 100 and 105. Additionally two subinterfaces have been added in the DMZ zone, VLAN 200 and 210. The eth1 interface is configured in Untrust zone. Policies can be written to allow or deny traffic between zones.

Figure 3-2 Security Zones and Interfaces



There are four default security zones configured on the appliance that you cannot delete:

- **Trust**—The trust zone is commonly used to segment internal networks from the wide area network (WAN) and Demilitarized Zone (DMZ).
- **Untrust**—The untrust zone is commonly used for the WAN. The untrust zone has default security enabled to prevent Denial of Service Attacks (DoS).
- **DMZ—**The DMZ zone is commonly used to segment publicly accessible servers from the local area network (LAN) and WAN.
- **Global—**The global zone is used to apply policies independent of zones.

Figure 3-3 displays the security appliance with two security zones: trust and untrust. The trust zone is configured for the LAN and the untrust zone is configured for the WAN. Security policies can now enforce access control between the two zones.

Figure 3-3 Security Zone (Trust and Untrust)

In addition to the four default zones, additional custom zones (refer to Figure 3-4) can be created to further divide the internal network into more granular segments.

Figure 3-4 Custom Security Zones

3.2 CREATING AND MODIFYING CUSTOM SECURITY ZONES

This section describes how to create, modify, and delete a custom security zone. This section includes the following topics:

- Creating Custom Security Zones
- Deleting Custom Security Zones
- Blocking Within a Zone
- Viewing Zone Configurations

3.2.1 CREATING CUSTOM SECURITY ZONES

Use the **set zone** command with the **name_str** option to create a custom security zone:

- set zone name {name_str}

Example: Creating the ”SALES” zone

- set zone name sales
- save

GUI Example: Creating the ”SALES” zone

- Network > Zone > Add Zone
- Create the following zone then click **Apply**:

Zone Name: Sales

3.2.2 DELETING CUSTOM SECURITY ZONES

Use the **unset zone** command to delete a security zone:

- unset zone {name_str}

Example: Deleting the “SALES” security zone

- unset zone sales
- save

GUI Example: Deleting the “SALES” security zone

- Network > Zone
- Remove the following zone then click **Apply**:

Zone Name: Sales

[NOTE] If a security zone is bound to an interface, you cannot delete the zone until you unbind it from the interface. For information about interface commands, refer to 3.3

CONFIGURING INTERFACES AND SUBINTERFACES.

3.2.3 BLOCKING WITHIN A ZONE

By default, all hosts within a security zone are allowed to communicate with each other. Intrazone blocking disables host-to-host communication within a security zone.

Use the **set zone** command with the **block** option to enable intrazone blocking on a specified security zone:

- set zone {name_str} block

Example: Enable Intrazone blocking on the “SALES” security zone.

- set zone sales block
- save

GUI Example: Enable Intrazone blocking on the “SALES” security zone.

- Network > Zone > Edit (for “Sales”)
- Check the following, then click **Apply:**
  Block Intra-Zone Communication

Use the **unset zone** command with the **block** option to disable intrazone blocking on a specified security zone:

- unset zone {name_str} block

Exampe: Disabling Intrazone blocking on the “SALES” security zone.

- unset zone sales block
- save

GUI Example: Disabling Intrazone blocking on the “SALES” security zone.

- Network > Zone > Edit (for “Sales”)

- Uncheck the following, then click **Apply**:
  Block Intra-Zone Communication

3.2.4 VIEWING ZONE CONFIGURATIONS

Use the **get zone** command to display information on all security zones. The following information appears for each zone:

- **Zone name**—The name assigned to the interface.
- **Zone ID**—The ID number assigned to the zone.
- **Type**—The security settings on the zone.
- Intrazone block—On or off.
- **Interfaces bound**—Lists all physical and logical interfaces bound to the zone.

Use the get zone command to display information on a specific zone:

- get zone {interface name}

Use the get zone all command to display information on all zones:

- get zone all

Figure 1-1 shows an example of the **get zone** command.

```
cli-> get zone
                    ID: 0   Type: Pre-defined
Zone: global        Intra-zone block: Off  Flags: IcmpFrag IcmpLarge FinNoAck
SynFlood: 65535     FinFlood: 65535     IcmpFlood: 16777215  FragFlood: 16777215

                    ID: 1   Type: Pre-defined
Zone: dmz           Intra-zone block: Off  Flags: IcmpFrag IcmpLarge FinNoAck
SynFlood: 65535     FinFlood: 65535     IcmpFlood: 16777215  FragFlood: 16777215

                    ID: 2   Type: Pre-defined
Zone: untrust       Intra-zone block: Off  Flags: IcmpFrag IcmpLarge FinNoAck
SynFlood: 65535     FinFlood: 65535     IcmpFlood: 16777215  FragFlood: 16777215

                    ID: 3   Type: Pre-defined
Zone: trust         Intra-zone block: Off  Flags: IcmpFrag IcmpLarge FinNoAck
SynFlood: 65535     FinFlood: 65535     IcmpFlood: 16777215  FragFlood: 16777215
```

Figure 3-5 Get Zone Command Example

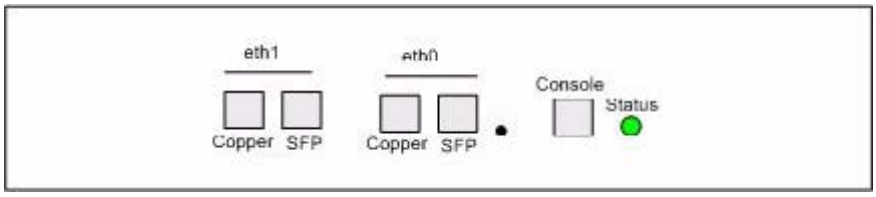
GUI Example: Get Zone

- Network > Zone > Zone Table
  Shows current zones available for configuration

3.3 CONFIGURING INTERFACES AND SUBINTERFACES

Each physical interface on the security appliance supports up to 100 virtual LANs (VLANs) for a maximum of 200 total per appliance on two-port appliances, and 240 on appliances with more than two ports. To route VLAN traffic through the security appliance, a subinterface is required. For every VLAN, a subinterface is configured on the corresponding physical interface of the appliance. Figure 3-6 displays the location of the eth0 and eth1 interfaces on the <NetSecure 6100>.

Figure 3-6 Eth0 and Eth1 Locations



This section describes the commands used to configure interfaces, bind them to a security zone, and move them between zones. This section also describes performing the same tasks with subinterfaces.

This section includes the following topics:

- Configuring Interfaces
- Binding Interfaces to a Security Zone
- Moving Interfaces between Security Zones
- Configuring Subinterfaces
- Deleting Subinterfaces

3.3.1 CONFIGURING INTERFACES

Use the **set interface** command with the **ip** option to assign an IP address and netmask to the interfaces on the appliance:

- set interface {interface name} ip {ip_addr/mask}

Example: Configuring the ETH0 interface with the IP address 10.0.0.1/24

- set interface eth0 ip 10.0.0.1/24
- save

GUI Example: Configuring the ETH0 interface with the IP address 10.0.0.1/24

- Network > Interface > Edit (eth0)
- Enter the following address information then click **Apply**:
  Type Interface IP: 10.0.0.1
  Type Netmask: 24

By default, the interface belongs to the trust zone and is placed in route mode. Refer to Configuring Interface Modes for additional information. You can use additional **set interface** commands to bind the interface to a different zone or to set the interface mode to either NAT-enabled, route or Transparent mode.

3.3.2 BINDING INTERFACES TO A SECURITY ZONE

All physical and logical interfaces must bind to a security zone. Inbound and outbound security policies are applied to the source and destination zone and encompass all interfaces that are members of those security zones.

Use the **set interface** command with the **zone** option to bind an interface to a security zone:

- set interface {interface name} zone {name_str}

Example: Binding the ETH0 interface to the “SALES” security zone

- set interface eth0 zone sales
- save

GUI Example: Binding the ETH0 interface to the “SALES” security zone

- Network > Interface > Edit (for eth0)

- Select the following, then click **Apply**:
  Zone Name: Sales

3.3.3 MOVING INTERFACES BETWEEN SECURITY ZONES

Unbinding an interface removes the interface from the assigned zone and places it into the zone specified in the **set interface** command. To move an interface from one assigned zone to another, use the **set interface** command and assign the interface to the new zone. The new zone policies are enforced to the specified interface.

Example: Moving the ETH0 Interface to the trust security zone.

- set interface eth0 zone trust
- save

GUI Example: Moving the ETH0 Interface to the trust security zone.

- Network > Interface > Edit (for eth0)
- Select the following, then click Apply:
  Zone Name: Trust

3.3.4 CONFIGURING SUBINTERFACES

A subinterface is a logical interface that uses an 802.1q tag to identify membership to a specific VLAN on a physical interface. After you configure a subinterface and assign it to a zone, traffic can pass from VLANs associated with the subinterface to other physical or logical interfaces on the appliance. Additionally, security policies assigned to a zone containing a subinterface enforces that policy on all traffic to and from that subinterface.

The interface name that refers to the subinterface has the following format:

{physical interface name.vlan_id}

For example, interface eth0.125 is the subinterface for the VLAN with VLAN id 125 located on the eth0 physical interface.

Use the **set interface** command to bind a subinterface to a physical interface. You must specify the **vlan_id** that defines the 802.1q tag. The name of the physical interface associated with the VLAN ID and subinterface IP address are required to create the subinterface.

set interface {physical interface name.vlan_id} ip {ip_addr/mask}

[NOTE] The vlan_id must fall within the range of 1 to 4000.

Once the subinterface is created, use the set interface command to add the subinterface to a zone:

set interface {interface name} zone {name_str}

Example: Configuring a subinterface with IP address and zone.

Use the set interface command to create a subinterface for the VLAN with VLAN id 120 on the physical interface eth0. Assign the subinterface to the trust zone with the IP address 192.168.100.1/24:

- set interface eth0.120 ip 192.168.100.1/24
- set interface eth0.120 zone trust
- save

GUI Example: Configuring a subinterface with IP address and zone.

- Network > Interface > Edit (for eth0)
- Enter the following, then click Apply:
  VLAN ID: 120
  IP Address/Netmask: 192.168.100.1/24
  Zone Name: Trust

3.3.5 DELETING SUBINTERFACES

You must remove all policies bound to a subinterface before you can delete a subinterface. After you remove all policies, use the **unset interface** command to delete the subinterface:

unset interface {interface name}

Example: Deleting the subinterface ETH0.120

- unset interface eth0.120
- save

GUI Example: Deleting the subinterface ETH0.120

- Network > Interface > Remove (for eth0.120)
- Select the following:
  Are you sure you want to remove: Yes

3.4 CONFIGURING INTERFACE MODES

You can configure interfaces with one of thre interface modes that determine whether the source IP address of traffic is translated to the IP address of the egress interface. The thre interface modes are NAT-enabled, route and transparent mode. You can configure additional NAT policies, such as one-to-one NAT, many-to-one NAT, many-to-many NAT and port address translation (PAT), through security policies. For information on configuring NAT through security policies, refer to Chapter 10 Address Translation.

3.4.1 CONFIGURING NAT-ENABLED MODE

Interfaces configured with NAT-enabled mode translate the source IP address of all traffic to the IP address of the egress interface. This configuration enables the appliance to hide the IP addresses of hosts on the interface configured in NAT-enabled mode from remote hosts.

Use the **set interface** command with the **nat** option to configure NAT-enabled mode on an interface:

set interface {interface name} nat

displays a network diagram of an appliance with the eth0 interface configured in NAT-enabled mode. When a host on the eth0 interface needs access to information located on the Internet, the source IP address of all traffic from that host is translated to the IP address of

the egress interface. In this case, the new translated source IP address is 128.196.10.2.

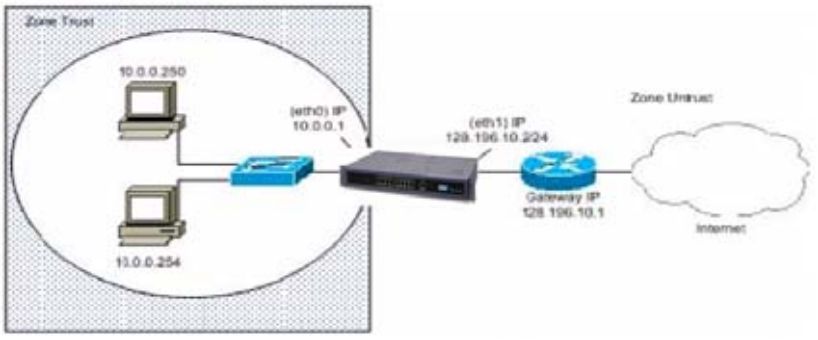


Figure 3-7 NAT-Enabled Mode

Example: Configuring NAT-Enabled Mode

configure NAT-enabled mode on the eth0 interface of the appliance in:

- set interface eth0 nat
- save

GUI Example: Configuring NAT-Enabled Mode

- Network > Interface > Edit (for eth0)
- Enter the following, then click Apply:
  Interface Mode: NAT

3.4.2 CONFIGURING ROUTE MODE

Route mode maintains the source IP address of all traffic as it traverses across interfaces. Route mode requires that all interfaces have a unique IP address and netmask. By default, all newly configured interfaces are in route mode.

Use the **set interface** command with the **route** option to configure route mode on an interface:

set interface {interface name} route

[NOTE] To change the interface mode from NAT Mode to Route Mode, use the **set interface (interface name) route.**

Example: Configure Route mode

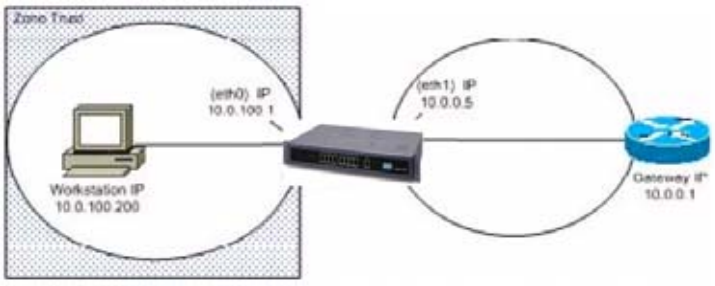
Configure route mode on the eth0 and eth1 interfaces of the appliance displayed in Figure 3-8 :

- set interface eth0 route
- set interface eth1 route
- save

GUI Example: Configure Route mode

- Network > Interface > Edit (for eth0)
- Enter the following, then click **Apply**:
  Interface Mode: Route
- Network > Interface > Edit (for eth1)
- Enter the following, then click **Apply**:
  Interface Mode: Route

Figure 3-8 Route Mode



All traffic from eth0 to eth1 and from eth1 to eth0 maintains their original source IP addresses.

3.4.3 VIEWING INTERFACE INFORMATION

Use the **get interface** command to display interface information. The following information appears for each physical and logical interface:

- **Name**—The name assigned to the interface.
- **IP address/subnet**—The IP address and subnet assigned to the interface.
- **Zone**—The zone assigned to the interface.
- **Media Access Control (MAC) Address**—The MAC address assigned to the interface.
- **VLAN**—Identifies any VLANs configured on the interface.
- **Status**—Shows the link status of an interface as either U (up) or D (down).
- **MTU Size**—Displays the current MTU size set for the interface.
- **Manage IP**—Shows the IP address from which the interface can be managed.
- **Management Options**—Ping, ssh, http, https, snmp
- **Mode**—NAT, route, transparent

Use the **get interface** command to display information on a specific interface:

get interface {interface name}

Use the **get interface all** command to display information on all interfaces:

get interface all

Example: Get Interface ETH0

- cli-> get int eth0
- if_index 1, mode route
- admin status up, link status up
- mtu 1500

- configured type copper, speed auto, mode full-duplex
- negotiated type copper, speed 1000, mode full-duplex
- ip 192.168.65.49/24, mac 0060.2620.0094
- manage ip 0.0.0.0, mac 0060.2620.0094
- ping disabled, SSH disabled, HTTP enabled, HTTPS enabled, SNMP disabled
- Telnet disabled, DHCP disabled
- zone global

GUI Example: Get Interface ETH0

- Network > Interface > Edit (for ETH0)
- Displays interface for ETH0

3.4.4 CONFIGURING TRANSPARENT MODE

This section describes the Transparent Mode feature. It includes the following topics:

- Transparent Mode Overview
- Transparent Mode Simple Deployment
- Transparent Mode Simple ACL Functions

3.4.4.1 TRANSPARENT MODE OVERVIEW

When the <NetSecure 6100> is configured to run in Transparent mode the device is configured with the same network on both interfaces. In this mode the <NetSecure 6100> functions like a layer 2 switch or bridge. As packets traverse through the firewall they will do so without having their src/dest IP/MAC address information changed in the header, allowing the <NetSecure 6100> to be deployed in complex networks un-obtrusively.

In Transparent mode the <NetSecure 6100> can be deployed deep within a core

network as it will pass all traffic without additional configuration. All routing protocols, and broadcast protocols can be passed seamlessly through the <NetSecure 6100>. While in this mode the <NetSecure 6100> can be further configured to bypass various network security functions that in some cases are not desired by the network/security administrator.

In addition to passing various protocols without interception, the <NetSecure 6100> Transparent mode supports VLAN (802.1q) recognition and filtering. If desired, the <NetSecure 6100> can be deployed into an existing VLAN network, and be configured to recognize the various 802.1q packets and apply traffic policies using its zone-based filter. This function is called Transparent-VLAN filtering and is described in 3.4.4.2.2 Transparent Mode VLAN Filtering.

3.4.4.2 TRANSPARENT MODE SIMPLE DEPLOYMENT

In Figure 3-9 the <NetSecure 6100> is deployed as a transparent mode firewall. Interface eth0 and eth1 are configured in transparent mode with the address of 0.0.0.0. Interface eth0 is configured in the Trust Zone and eth1 will assigned to the Untrust zone. A policy configured to any from the Trust zone to the Untrust zone. To restrict external traffic from accessing the Trust zone, a policy will be needed to deny ANY/All from the Untrust to Trust zone.

In Figure 3-9, if Workstation A makes a request to www.yahoo.com, the workstation performs a DNS query for www.yahoo.com, the return address for the site will be a routable Internet address. The host then performs an arp for its default gateway and sends the packet to the router 10.0.0.1. The <NetSecure 6100> inspects the outgoing request and runs the packet through its Policy engine. Due to the permit policy created earlier, this packet will be left intact and allowed out through the eth1 interface of the <NetSecure 6100>. During the inspection process a session is added for this packet meaning the return packet will be flagged as a valid "trust" packet.

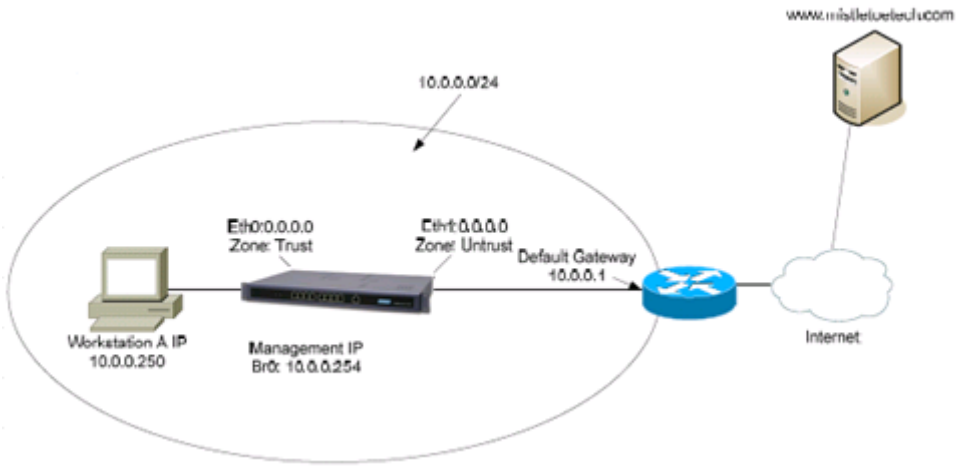


Figure 3-9 Transparent Mode

3.4.4.2.1 Transparent Mode Management

In order to manage the <NetSecure 6100> through the network, you must configure a management interface. In Transparent mode, the logical management interface, br0, is utilized.

[NOTE] On the 2-port appliances, br0 represents both eth0 and eth1 as a logical interface and is specifically designed to be used for management traffic while in Transparent mode.

[NOTE] On all other appliances with 8 ports, this translates to 4 bridge ports. br0 (eth0 and eth4), br1 (eth1 and eth5), br2 (eth2 and eth6), and br3 (eth3 and eth7). These ports can configured independently (eth0 and eth4 in Transparent mode, eth1/2/3/5/6/7 in Route/Nat mode or you can configure all 4 bridge ports in a complex Transparent mode design). These bridge-to-ports assignments are hard-coded within the appliance and cannot be modified.

In addition to configuring the br0 management interface, a default route is required to be configured in order for the <NetSecure 6100> to communicate to host/s that are outside its immediate network subnet. For example if SNMP or SSH is required from a host that is somewhere on the Internet, the <NetSecure 6100> will need a route configured to the default gateway. If the host requesting the management traffic exists somewhere deep within the LAN network, a static route may have to be added.

Note: br0 responds to request on both the Untrust and Trust zone and therefore if

filtering of the management request is required then the Manage-ip function should be used.

Following is the CLI example for Figure 3-9:

- set zone name Accounting
- set zone name Finance
- set interface eth0 ip 0.0.0.0/0
- set interface eth0 transparent
- set interface eth0 zone trust
- set interface eth1 ip 0.0.0.0/0
- set interface eth1 transparent
- set interface eth1 zone untrust
- set interface br0 ip 10.0.0.254/24
- set interface br0 manage ping
- set route 0.0.0.0/0 interface br0 gateway 10.0.0.1
- set policy from trust to untrust any any any permit
- set policy from untrust to trust any any any deny

3.4.4.2.2 Transparent Mode VLAN Filtering

Some network administrators desire the ability to apply security policies between various VLAN networks. Due to the performance hit that most L3 switches take when doing L3/L4 ACL filtering administrators are less likely to utilize their core switches for such task. The <NetSecure 6100> can be deployed in such environments and be utilized as a VLAN policy enforcer.

The <NetSecure 6100> can be placed directly between the VLAN switch/trunk and the external VLAN router, it can then intercept/recognize various VLAN tagged packets and apply zone based policies to these types of traffic. This is possible through the additional lookup parameter activated in the Policy engine when configured in this mode. The VLAN tag id which is bound to a zone and through proper configuration, prompts the <NetSecure 6100> to inspect the VLAN

traffic and be on the lookout for the 802.1q header. The <NetSecure 6100> then correlates the q tag to the configured Zone and applies the policy engine to this packet.

In Figure 3-10, the <NetSecure 6100> is deployed in an environment with 5 existing VLAN networks which represents 5 different departmental networks:

- VLAN 100: Engineer
- VLAN 200: Accounting
- VLAN 300: Finance
- VLAN 400: Lab
- VLAN 500: Sales.

To further secure management traffic, an additional VLAN network is created solely for management access. This is done by creating a sub-interface for br0. In this scenario we will create a VLAN called br0.5.

Figure 3-10: Transparent Mode with VLAN Filtering

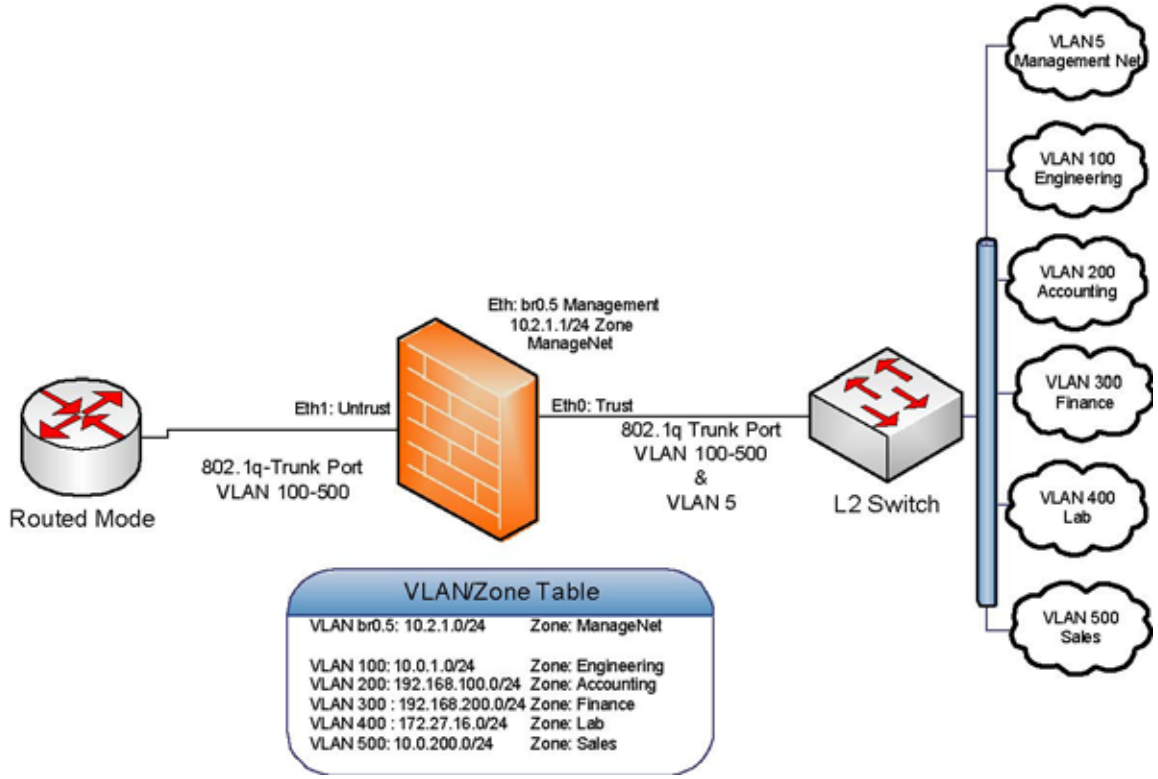


Figure 3-10 Transparent Mode with VLAN Filtering

In Figure 3-10 the <NetSecure 6100> will be in Transparent mode with multiple

VLAN interfaces and Zones. This will give an administrator the ability to filter various source/dest address's/zones based on the VLAN ID.

3.4.4.2.3 CLI Configuration

- set interface eth0 ip 0.0.0.0/0
- set interface eth0 transparent
- set interface eth0 zone trust
- set interface eth1 ip 0.0.0.0/0
- set interface eth0 transparent
- set interface eth1 zone untrust

- set interface br0.5 ip 10.2.1.1/24
- set interface br0.5 zone ManageNet
- set interface br0.5 manage ssh/ping
- set route 0.0.0.0/0 interface br0 gateway

- unset transparent bypass-vlan-policy

- set zone name ManageNet
- set zone name Engineering
- set zone name Accounting
- set zone name Finance
- set zone name Lab
- set zone name Sales

- set address Finance webserver 192.168.200.10/32
  set address Accounting SQLServer 192.168.100.100/32

- set transparent vlan Engineering tag 100 zone Engineering
- set transparent vlan Accounting tag 200 zone Accounting
- set transparent vlan Finance tag 300 zone Finance
- set transparent vlan Lab tag 400 zone Lab
- set transparent vlan Sales tag 500 zone Sales
- set transparent vlan ManageNet tag 5 zone ManageNet

- set policy from Engineering to Lab any any any permit

- set policy from Lab to Engineering any any ssh permit
- set policy from Sale to Finance any webserver http permit
- set policy from Sales to Accounting any SQL sql permit

3.4.4.3 TRANSPARENT MODE SIMPLE ACL FUNCTIONS

As firewalls are placed deeper within high-speed transmission points, many network integrators are looking for simple methods of applying ACL's to specific types of traffic without causing disruption to their existing network topology. ISP's and Telco's are seeking methods to restrict various protocols or IP address traversing their central network while maintaining high transmission speeds.

Due to the nature of firewalls and packet filters, the option of enabling and disabling various security functions is somewhat limited. The <NetSecure 6100> provides the network administrator the option to bypass various security functions on the <NetSecure 6100> in order to accommodate their network needs.

These bypass functions are global and will be applied to both the ingress and egress interfaces.

[NOTE] For detailed information on the transparent commands used in the following examples, see the CLI Reference Guide.

3.4.4.3.1 Ability to bypass/pass MPLS packets

unset transparent bypass-mpls

This command will allow MPLS packets to traverse the <NetSecure 6100>. The default function of the <NetSecure 6100> is to bypass (i.e., drop) such packets.

GUI Example: Pass MPLS packets in transparent mode.

- Policy > Advanced > Bypass
- De-select the MPLS option and click Apply.

3.4.4.3.2 Ability to bypass/pass Unicast packets

unset transparent bypass-unicast

This command allows the bridging of non-IP unicast packets. The default behavior of the <NetSecure 6100> is to bypass (i.e., drop) such packets.

GUI Example: Pass UNICAST packets in transparent mode.

- Policy > Advanced > Bypass
- De-select the Non-IP Unicast option and click **Apply**.

3.4.4.3.3 Ability to bypass/pass non-ip Broadcast/Multicast traffic

set transparent bypass-bmcast

This command will bypass (i.e., drop) non-ip broadcast and multicast packets. The default behavior of the <NetSecure 6100> is to pass (i.e. allow) such packets.

GUI Example: Pass NON-IP Brodcast packets in transparent mode.

Check the Non-IP Broadcast option and click **Apply**.

3.4.4.3.4 Ability to bypass/pass DDOS traffic

unset transparent bypass-ddos

This command allows DDOS attacks and packets to traverse the <NetSecure

6100>. The default behavior of the <NetSecure 6100> is to bypass (i.e., drop) such packets.

GUI Example: ByPass Dos and Ddos checking in transparent mode.

Check the DDoS option and click **Apply**.

3.4.4.3.5 Ability to bypass/pass VLAN Policy filtering

unset transparent bypass-vlan-policy

This command will enable the Transparent-VLAN function covered in 3.4.4.2.2 Transparent Mode VLAN Filtering. The default behavior is to use the source physical ingress port for source zone derivation.

3.5 ADVANCED INTERFACE SETTINGS

If you choose to use advanced interface settings, you can modify the following elements of the security appliance:

- Configuring Maximum Transmission Unit (MTU) Settings
- Configuring Interface Link Up/Down
- Configuring Address Resolution Protocol (ARP)
- Enabling Interface Management
- Disabling Interface Management
- Setting the Interface Speed

3.5.1 CONFIGURING MAXIMUM TRANSMISSION UNIT (MTU) SETTINGS

The Maximum Transmission Unit (MTU) is the largest IP datagram that can be transferred using a specific link. If a packet exceeds the MTU size set on a specific interface, the network device can fragment the packet or, if permitted, send a Path MTU request to the host in question. The host should accept the request and send smaller packets that do not exceed the MTU limit. You can only configure MTU settings on the physical interfaces of the appliance.

Use the **set interface** command with the **mtu** option to set the MTU size for a specific interface:

set interface {interface name} mtu {size}

Example: Settingt the MTU size on theETH1 interface to 1450

- set interface eth1 mtu 1450
- save

GUI Example: Settingt the MTU size on theETH1 interface to 1450

- Network > Interface > Edit (for eth1)
- Enter the following, then click **Apply**:
  Maximum Transfer Unit (MTU): 1450

[NOTE] The default MTU size set for each interface is 1500. It is recommended that the MTU size on the eth1 interface matches the MTU size of the next hop router.

3.5.2 CONFIGURING INTERFACE LINK UP/DOWN

Use the **set interface** command with the **phy** option to set the state of any physical or logical interface to up or down:

- set interface {interface name} phy link-up
- set interface {interface name} phy link-down

Example: Changing the ETH0 interface state to "Down"

set interface eth0 phy link-down

Example: Changing the ETH0 interface state to "UP"

set interface eth0 phy link-up

3.5.3 CONFIGURING ADDRESS RESOLUTION PROTOCOL (ARP)

The <NetSecure 6100> keeps an active list of all hosts directly connected to any physical or logical interface in its ARP table. This table includes the hosts IP address and Media Access Control (MAC) addresses.

Use the **get arp** command to view the current ARP table entries:

get arp

3.5.3.1 CLEARING CURRENT ARP ENTRIES

Use the **clear arp** command to clear a specific entry or all current ARP entries:

clear arp {ip_addr| all}

3.5.3.2 ADDING STATIC ARP ENTRIES

Use the **set arp** command to add a static ARP entry:

set arp {ip_addr} {mac_addr }

Example: Adding a static ARP entry

Use the set arp command to add a static ARP entry for a host connected on the eth0 interface with an IP address of 10.0.0.1 and a MAC address of aa:bb:cc:dd:ee:ff:

- set arp 10.0.0.1 aabbccddeeff
- save

GUI Example: Adding a static ARP entry

- Network > ARP Add
- Enter the following, then click **Apply**:
  IP Address: 10.0.0.1
  MAC Address: aabbccddeeff
  Interface: ETH0

3.5.3.3 DELETING STATIC ARP ENTRIES

Use the **unset arp** command to remove a static ARP entry:

unset arp {ip_addr} {mac_addr}

3.5.3.4 SETTING THE ARP TIMEOUT

The default timeout for all ARP entries is 5000 seconds. Use the **set arp age** command to increase or decrease the allowed ARP timeout:

set arp age {number}

Example: Setting the ARP TIMEOUT to 1800 seconds

- set arp age 1800
- save

GUI Example: Setting the ARP TIMEOUT to 1800 seconds

- Network > ARP
- Enter the following, then click Apply:
  ARP Cache Entry Timeout (Seconds): 1800

3.5.3.5 ENABLING INTERFACE MANAGEMENT

Use the set interface {interface name} with the management option to turn on the specific interface management options.

set interface {interface name} manage {http|https|ping|snmp|ssh}

3.5.3.6 DISABLING INTERFACE MANAGEMENT

Use the unset interface {interface name} with the management option to turn off the specific interface management options.

Example: Allow the ETH0 interface to respond to PING

set interface eth0 manage ping

GUI Example: Allow the ETH0 interface to respond to PING

- Network > Interface > Edit (for eth0)

- Select the following, then click **Apply**:
  Management Option: Ping

3.5.3.7 SETTING THE INTERFACE SPEED

When you configure the <NetSecure 6100>, the interface auto-negotiates to 1000Mbps. To set the interface to support 100Mbps or 10Mbps, use the **set interface** command with the **speed** option.

set interface {interface name} speed {100Mb|10Mb|auto}

[NOTE] 100Mbps and 10Mbps half duplex are not supported.

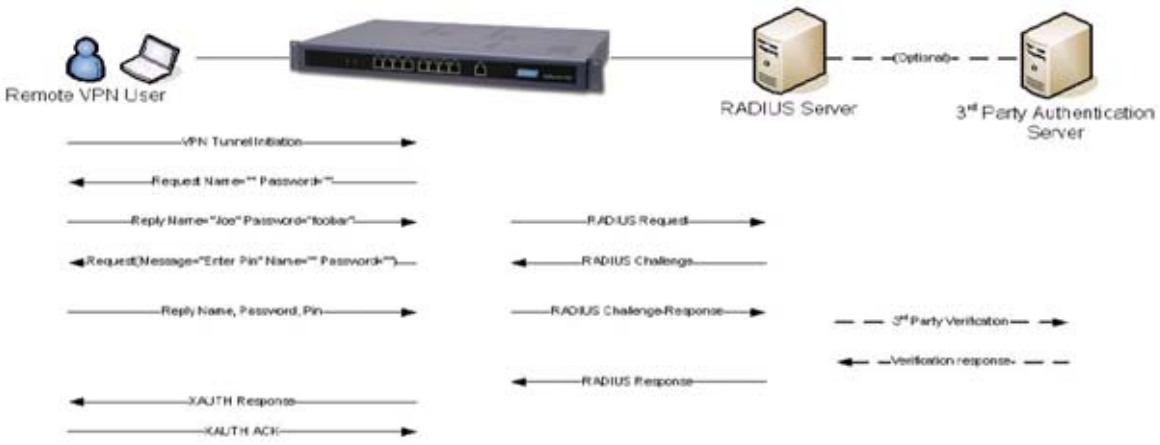
3.6 AUTHENTICATION USING RADIUS

Remote Authentication Dial-In User Service (RADIUS) authenticates the local users and remote users on a company network. RADIUS works as a client/server system that keeps the authentication information for users, remote access servers, and VPN gateways in one database. The authentication messages between the RADIUS client and the RADIUS server always use an authentication key. This authentication key, or shared secret, must be configured the same on both the RADIUS server and client. Without this key, hackers cannot get to the authentication messages.

3.6.1 HOW THE RADIUS CHALLENGE-RESPONSE MODE WORKS

In the RADIUS Challenge-Response mode, there is an additional Challenge-Response sequence of messages before the successful completion of user authentication. The following example illustrates the Challenge-Response authentication mode with RADIUS (Figure 3-11).

Figure 3-11 RADIUS Challenge Response Message Exchange



1. User tries to establish a VPN Tunnel with the security appliance

2. The security appliance prompts the remote user for a username and password.

3. User provides his username and password to the security appliance.

4. The security appliance queries the RADIUS server to verify the authentication.

5. The RADIUS server verifies the username and password and if they are correct.sends a RADIUS Challenge message to the security appliance.

6. The security appliance sends the Challenge message to the user.

7. User responds to the Challenge question by entering other information (in thisexample a Pin code).

8. The RADIUS server can be used to authenticate the pin code itself, or optionally use a 3rd party authentication server to authenticate the pin code. In this example there is a 3rd party server, and the RADIUS server connects to the 3rd party to verify the pin code.

9. The 3rd party server verifies the pin code and gives verification response.

10. The RADIUS server sends RADIUS Response to the security appliance.

11. The security appliance sends XAUTH response to User VPN Client.

12. User VPN Client acknowledges.

3.6.2 RADIUS CLIENT ATTRIBUTES

To allow the RADIUS client to interact with the RADIUS server the proper attributes must be configured on both the RADIUS client and server. These attributes include:

Auth_Name—Allows all the RADIUS attributes to be configured into a single RADIUS group.

RADIUS Server Name—The IP address or DNS name of the RADIUS server.

RADIUS Shared Secret—A shared secret must be configured on the security appliance and the server to allow encrypted communication.

RADIUS Port—The port number on which the RADIUS server is listening. The default RADIUS port used by the security appliance is 1812.

RADIUS Timeout—The time interval the security appliance must wait before sending another authentication request if the previous request had not been answered. The default RADIUS timeout value for the security appliance is 3 seconds.

RADIUS Retry—he number of retries the RADIUS client will send to the RADIUS server. The default RADIUS retry value for the security appliance is 1.

RADIUS SRC-Interface—The source interface from which the security appliance will send the RADIUS requests.

3.6.2.1 CONFIGURING THE RADIUS SERVER NAME

To configure the RADIUS server name use the **set auth-server** command with the **server-name** option.

- set auth-server {auth_name} server-name {ip_addr|
- dom_name}

3.6.2.2 DELETING THE RADIUS SERVER NAME

To delete the RADIUS server name use **the unset auth-server** command and specify the auth_name used to configure the RADIUS server name.

unset auth-server {auth_name}

3.6.2.3 CONFIGURING THE RADIUS SHARED SECRET

To configure the RADIUS shared secret use the **set auth-server radius** command with the **secret** option.

set auth server {auth_name} radius secret {password_str}

3.6.2.4 CONFIGURING THE RADIUS PORT

To configure the RADIUS port use the **set auth-server radius** command with the **port** option.

set auth-server {auth_name} radius port {value}

[NOTE] The acceptable value for the RADIUS port is in the range 102465535.

3.6.2.5 CONFIGURING THE RADIUS TIMEOUT

To configure the RADIUS Retry Timeout use the **set auth-server radius** command with the **timeout** option.

set auth-server {auth_name} radius timeout {value}

[NOTE] The acceptable value for the RADIUS timeout is in the range of 3-180 seconds.

3.6.2.6 CONFIGURING THE RADIUS RETRY

To configure the RADIUS Retry use the **set auth-server radius** command with the **retries** option.

set auth-server {auth_name} radius retries {value}

[NOTE] The acceptable value for the retry is in the range 1-30.

3.6.2.7 CONFIGURING THE RADIUS SRC-INTERFACE

To allow the security appliance to communicate with the RADIUS server a source interface must be specified. To configure the RADIUS SRC-Interface use the **set auth-server** command with **the src-interface** option.

set auth-server {auth_name} src-interface {interface name}

3.6.3 RADIUS BACKUP SERVER

In addition to the primary RADIUS server two additional RADIUS servers can be defined, enabling the security appliance with a backup RADIUS server option if the primary RADIUS server were to fail and become unresponsive. This allows users to continue authentication into the network.

Backup1—IP Address or domain name of primary backup server.

Backup2—IP Address or domain name of secondary backup server.

3.6.3.1 CONFIGURING THE RADIUS BACKUP SERVER

To configure the RADIUS backup server use the **set auth-server** command with the **backup** option.

set auth-server {auth_name}{backup1| backup2}{ip_addr| dom_name}

3.6.3.2 VIEWING THE RADIUS CONFIGURATION

To view the RADIUS configuration on the security appliance use the get auth-server command and view all settings or by ID.

get auth-server {all| id}

Example: View the RADIUS configuration using the all option.

```
cli-> get auth-server all
ID   Auth Server   Server Name        Type          Acct Type     Role
-------------------------------------------------------------------------------

0    RADIUS        192.168.1.100      RADIUS        xauth         -cli->
```

GUI Example: View the currentRADIUS configuration

System > Authentication > Authentication Server

Shows all Radius server configurations

Example: View the RADIUS configuration by specifying the ID 0.

- cli-> get auth-server id 0
- ID: 0 AuthServer: RADIUS
- Type: RADIUS Server Name/IP: 192.168.1.100
- Backup1: Backup2:
- Timeout: 3 Account Type: xauth
- Source Interface:
- RADIUS shared secret: test
- RADIUS server port: 1812
- RADIUS # of retry : 1
- cli->

Figure 3-12 shows a primary and secondary RADIUS server using the following attributes:

Figure 3-12 Configuring a Primary and Secondary RADIUS Server

- **Auth_name:** security
- Primary RADIUS server IP—10.0.0.250
- Secondary RADIUS server IP—10.0.0.251
- RADIUS Shared Secret—password
- RADIUS Timeout—5
- RADIUS Port—1850
- RADIUS Retry—3

- RADIUS SRC-Interface—eth0

To configure the following RADIUS attributes follow these steps:set auth server security server-name 10.0.0.250

- set auth-server security backup1 10.0.0.251
- set auth-server security radius secret password
- set auth-server security radius timeout 5
- set auth-server security radius port 1850
- set auth-server security radius retries 3
- set auth-server security src-interface eth0
- save

GUI Example: Configuring a Primary and Secondary RADIUS server

1. System > Authentication > Add Authentication Server
2. Enter the following RADIUS information and click Apply:
   - Type Name: Test
   - Type IP/Domain: 10.0.0.250
   - Type backup1: 10.0.0.251
   - Type shared secret: password
   - Type RADIUS port: 1850
   - Type RADIUS timeout: 5
   - Type number of retries : 3
3. Select the eth0 interface

To view the RADIUS server settings use the **get auth-server id 0** command.

- cli-> get auth-server id 0
- ID: 0 AuthServer: security

- Type: RADIUS Server Name/IP: 10.0.0.250
- Backup1: 10.0.0.251 Backup2:
- Timeout: 5 Account Type: xauth
- Source Interface: eth0
- RADIUS shared secret: password
- RADIUS server port: 1850
- RADIUS # of retry : 3
- cli->

3.7 ALTERNATE CONNECTION METHODS

3.7.1 PPPoE: POINT -TO-POINT PROTOCOL OVER ETHERNET

PPPoE lets Internet Service Providers (ISPs) use their existing Radius authentication systems from their Dial-Up service on a Broadband / Ethernet-based service. Since Dial-Up is PPP and most broadband connections are Ethernet, Point to Point Protocol over Ethernet (PPPoE) merges the Point-to-Point Protocol (PPP) with the Ethernet protocol.

Many users can share the same physical connection, but access control, billing, and type of service are handled on a per-user basis. Some security devices support a PPPoE client, allowing compatibly with DSL, Ethernet Direct, and cable networks run by ISPs using PPPoE for client Internet access.

3.7.2 SETTING UP PPPoE

The following example illustrates how to define the untrusted interface of a security device for PPPoE connections and how to initiate PPPoE service.

In this example, the security device receives a dynamically assigned IP address for its Untrust zone interface (eth1) from the ISP. In this case, the security device acts as a PPPoE client.

Before setting up the site in this example for PPPoE service, you must have the following:

- Digital subscriber line (DSL) modem and line
- Account with ISP
- Username and password (obtained from the ISP)

Every TCP/IP connection that a host in the Trust zone makes to the Untrust zone automatically goes through the PPPoE encapsulation process.

[NOTE] When enabling PPPoE, the trust interface must be in NAT or Route mode.

Example: To set interfaces and PPPoE

- set interface ethernet0 zone trust
- set interface ethernet0 ip 192.168.0.1/24
- set interface ethernet1 zone untrust
- set pppoe interface ethernet1
- set pppoe username *name_str* password *pswd_str*

To test your PPPoE connection:

- set pppoe enable
- get pppoe

GUI Example: To set interfaces and PPPoE

1. Network > PPPoE > Edit
2. Enter the following PPPoE information and click Apply:
   - Type Username: name
   - Type Password: password
   - Select PPPoE enable
3. Network > Interface > Edit eth0
4. Enter the following interface information and click Apply:
   - Select Zone: Trust
   - Select Interface Mode: NAT
   - Type IP Address: 192.168.0.1
   - Type Netmask: 24
5. Network > Interface > Edit eth1

6. Enter the following interface information and click Apply:

   - Select Zone: Untrust
   - Select Interface: PPPoE

Chapter 4. System Management

This chapter describes the management options for the <NetSecure 6100>, including software management, system management and user account management. The following topics are included in this chapter:

- Using the Console to Manage the <NetSecure 6100>
- Using SSH to Manage the <NetSecure 6100>
- Managing Users for the <NetSecure 6100>
- Managing Software for the <NetSecure 6100>
- Resetting and Restarting the <NetSecure 6100>
- Additional System Management Tasks
- Using Network Time Protocol (NTP)
- Using Domain Name Service (DNS)
- Using Ping
- Using Traceroute

4.1 USING THE CONSOLE TO MANAGE THE <NetSecure 6100>

You must perform initial configuration of the <NetSecure 6100> using the console interface. After you configure the <NetSecure 6100> for the first time, you can manage it through the console or using a secure shell (SSH). Refer to 4.2

USING SSH TO MANAGE THE <NetSecure 6100>.

This section describes how to work with the console and includes the following topics:

- About Console Cable Requirements
- Accessing the Console
- Re-enabling the Console Interface
- Viewing Console Interface Settings
- Setting the Console Display
- Setting the Console Timeout
- Exiting the Console

4.1.1 ABOUT CONSOLE CABLE REQUIREMENTS

Table 4-1 lists the required pin-out for the console cable used to manage the <NetSecure 6100>:

Table 4-1 Console Cable Pin-out

Female 2x5 Header	Female DB9
1	1
2	6
3	2
4	7
5	3
6	8
7	4
8	9
9	5
10	NC

4.1.2 ACCESSING THE CONSOLE

You must initially configure the <NetSecure 6100> through the console interface. For administration console access, you must connect the null modem cable included in the packaging to configure the <NetSecure 6100>.

4.1.2.1.1 To access the console:

1. Connect the female 2x5 header of the modem cable to the <NetSecure 6100>.

2. Connect the other female DB9 connector to a serial interface on the laptop or desktop machine.

3. To access the <NetSecure 6100> management interface you will need to launch a terminal emulation program. Hyper-Terminal by Hillgraeve Inc. is a suitable terminal emulation program and is included on most versions the Windows operating system. The default login credentials are admin and password.

4. Enter the following port settings:

   - Baud Rate—38,400
   - Parity—No
   - Data Bits—8
   - Stop Bits—1
   - Flow Control—None

5. Press Enter to see the login prompt.

6. At the login prompt, type admin.

7. At the password prompt, type admin.

[NOTE] If you log into the <NetSecure 6100> for the first time, use the default login credentials. If you changed your password, use the login name admin and your new password.

[NOTE] Information for long commands might display incorrectly if the console window is resized to larger than 80 character columns.

4.1.3 RE-ENABLING THE CONSOLE INTERFACE

To re-enable the console interface after it is disabled, use the **unset console** command:

unset console disable

4.1.4 VIEWING CONSOLE INTERFACE SETTINGS

To view current console interface settings, including users who are logged in and to display information for the console interface, use the **get console** command:

get console

4.1.5 SETTING THE CONSOLE DISPLAY

Use the **set console** command to set the number of lines to display without a break. If the page display number is set to 0, no page breaks are used when information is displayed. The default display number is 22 lines for each page.

set console page {number}

Example: Setting the Console Page display to 50

- set console page 50
- save

4.1.6 SETTING THE CONSOLE TIMEOUT

To set the inactivity value for the console interface, use the **set console** command with the timeout option. The timeout value is represented in minutes.

The default inactivity timeout is 10 minutes.

set console timeout {number}

Example: Setting the Console TIMEOUT to 15 minutes

- set console timeout 15
- save

4.1.7 EXITING THE CONSOLE

To exit the console, type **exit.**

4.2 USING SSH TO MANAGE THE <NetSecure 6100>

For secure remote management of the security appliance, use an SSH program such as SecureCRT from Van Dyke Technologies, Inc.

Before you can establish an SSH session with the appliance, you must generate an SSH host key and enable SSH on the specified interface as described in this section.

4.2.1 GENERATING SSH HOST KEYS

To encrypt an SSH session, use the **exec ssh** command to generate an SSH host key :

exec ssh gen-hostkey

4.2.2 ENABLE SSH GLOBALLY

After generating the SSH Hostkey, ssh must be enabled globally on the <NetSecure 6100>.

set ssh enable

4.2.3 ENABLING SSH ON A SPECIFIC INTERFACE

You can enable SSH management on any interface. To enable SSH on a specific interface, use **set ssh** command with the **interface** option:

set ssh enabled interface {interface name}

Example: Enabling SSH on the ETH0 interface

- set interface eth0 manage ssh

- save

GUI Example: Enabling SSH on the ETH0 interface

- Network > Interface > Edit (for ethernet0)
- Select the following, then click **Apply**:
  Management Option: SSH

Example: Enable SSH on a VLAN interface ETH0.100

- set ssh enabled interface eth0.100
- save

GUI Example: Enable SSH on a VLAN interface ETH0.100

- Network > Interface > Edit (for ethernet0.100)
- Select the following, then click **Apply**:
  Management Option: SSH

4.2.4 DISABLING SSH ON A SPECIFIC INTERFACE

To disable SSH on a specific interface, use the **unset ssh** command:

unset ssh enabled interface {interface name}

4.2.5 VIEWING SSH SETTINGS

To view users who log in using SSH or to view the host key currently used for SSH, use the **get ssh** command:

get ssh {host-key | report}

4.3 MANAGING USERS FOR THE < NetSecure 6100>

The <NetSecure 6100> has a single global administrator account with the user name “admin.” This account has the following administrative privileges:

- Manage the root system of the appliance.
- Add, remove, and manage all other administrators.
- Establish and manage virtual systems and assign physical or logical interfaces to them.
- Add, remove, and manage security zones.
- Assign interfaces to security zones.
- Perform asset recovery.
- Reset the device to its default settings.
- Update the firmware.
- Load configuration files.
- Clear all active sessions of additional read-only users.

4.3.1 CHANGING YOUR ADMINISTRATOR PASSWORD

Since all <NetSecure 6100> appliances come pre-configured with the same password, you must change the admin password to create a unique password for your organization. Use the **set admin** command:

set admin password {password_str}

[NOTE] You cannot change the administrator user name “admin.”

GUI Example: Changing the ADMINISTRATOR password

- System > Admin > Administrators

- Enter the following password information and click **Apply**:
  Select the admin user
  Type old password
  Type new password
  Confirm new password

4.3.2 ABOUT ADDITIONAL TYPES OF USERS

The security appliance can support one additional user, called “admin-r,” with read-only access to the management interface.

4.3.3 CHANGING THE ADMIN-R PASSWORD

To change the admin-r password, use the **set admin-r** command:

set admin-r password {password_str}

[NOTE] You cannot change the user name “admin-r.”

GUI Example: Changing the ADMIN-R password

- System > Admin > Administrators
- Enter the following password information and click **Apply**:
  Select the admin-r user
  Type old password
  Type new password
  Confirm new password

4.3.4 VIEWING CURRENT USERS

To view users currently logged into the administration console, use the get admin command:

get admin current-user

4.4 MANAGING SOFTWARE FOR THE < NetSecure 6100>

Before you upgrade the <NetSecure 6100> software, make sure that you have the following:

- You have root privilege to access the appliance.
- You have a console connection or SSH session to manage the appliance.
- You have an installed and running TFTP server on your computer.
- An Ethernet connection to the appliance exists (You use this connection to transfer software from the TFTP server to the <NetSecure 6100> flash memory).
- You saved the newest software image to the TFTP server.

4.4.1 STORING SOFTWARE IMAGE FILES IN FLASH MEMORY

The <NetSecure 6100> can store the following software image files in flash memory:

- New software image
- Currently saved software image
- Factory default software image

4.4.2 DOWNLOADING NEW SOFTWARE

Please contact your sales representative for latest software images.

4.4.3 UPLOADING NEW SOFTWARE

To upload new software for the <NetSecure 6100>:

1. Make sure you have the latest version of software for the appliance. This can be obtained from your sales representative.

2. Place a copy of the latest software for the appliance into the root directory of the TFTP server program.

3. Make sure a TFTP server is running on a PC and the appliance can access it.

4. Log in as admin on the appliance using an application such as SSH or HyperTerminal if directly connected through the console port.

5. On the appliance, enter save software from tftp ip_addr filename mos {pri | sec}, where the ip_addr is the IP address of your computer and filename is the file name of the appliance software. In addition you must specify either the primary or secondary image location (pri | sec). This will download the image from the TFTP server to the primary or secondary location.

6. After saving the image to either the primary or secondary slot, execute the set image nextboot pri command to set it as the active image.

7. Reset the appliance by executing the reset command and entering y at the prompt.

8. Log in to the appliance.

9. Use the get system command to verify the version of software loaded on the appliance.

4.4.4 SAVING MOS SOFTWARE TO FLASH MEMORY USING TFTP

Use the **save software** command to upload new mos software using TFTP.

- save software from tftp *ip_addr filenam*e
- mos {*pri* | *sec*}

4.4.5 SAVING BOOT SOFTWARE TO FLASH MEMORY USING TFTP

Use the **save software** command to upload new boot software using TFTP.

- save software from tftp *ip_addr filenam*e
- boot {*pri* | *sec*}

4.4.6 SETTING THE SOFTWARE AS PRIMARY OR SECONDARY

After you upload the new software image to the appliance, you must set the image as the primary or secondary software image. Use the **set image** command to set the software as primary or secondary.

set image mos {pri| sec}

GUI Example: Setting the software as PRIMARY or SECONDARY

- System > Software
- Select Nextboot for the primary or secondary software image

4.4.7 SAVING THE CONFIGURATION FILE FOR EXPORT

To save the current configuration file to your local workstation, use a TFTP server running locally on your machine and use the **save config** command:

save config from flash to tftp { ip_addr} filename

GUI Example: Saving the configuration file for EXPORT

- System > Configuration
- Type the TFTP Server Address
- Type the File Name
- Select the save configuration button

Example: Saving the configuration file for EXPORT

The following example saves the configuration file to a server at IP address *192.168.0.3* from the *eth0* interface with the filename *mttcurrent.txt*:

save config from flash to tftp 192.168.0.3 mttflash.txt

GUI Example: Saving the configuration file for EXPORT

- System > Configuration
- TFTP Server Address: 192.168.0.3
- File Name: mttflash.txt
- Select the save configuration button

4.4.8 VIEW THE RUNNING CONFIGURATION

To view the current running configuration stored on the flash, use the **get config** command.

get config

4.4.9 VIEW THE SAVED CONFIGURATION

To view the current saved configuration stored in the flash, use the **get config** command with the saved option.

get config saved

GUI Example: View the saved configuration

- System > Configuration
- Select the Display Configuration button

4.5 RESETTING AND RESTARTING THE < NetSecure 6100>

This section describes how to reset the appliance and associated hardware and software, as well as how to restart the <NetSecure 6100>. This section includes the following topics:

- Resetting the Appliance
- Resetting the Software
- Restarting the <NetSecure 6100>

4.5.1 RESETTING THE APPLIANCE

You can use one of the following methods to reset the appliance to its default configuration:

- If you have management access to the <NetSecure 6100>, use the **unset all** command to reset the appliance back to factory defaults.
- If you do not have management access, perform a hardware reset, which erases the firmware and system settings. Although the reset deletes the system configuration file, you can access the appliance using the default login credentials.

Performing a hardware reset to the <NetSecure 6100> removes the current firmware image along with the current configuration file. If you have not saved a backup configuration file to the local flash or a workstation on your network, you will have to reconfigure the <Security Applicance.

4.5.2 RESETTING THE SOFTWARE

Through the administration console, use the unset all command to reset the <NetSecure 6100> to factory default settings. This command erases the current configuration and returns the configuration file to factory default. A restart is required after unset all.

4.5.3 RESTARTING THE < NetSecure 6100>

Through the management interface, you can use the reset command to restart the <NetSecure 6100> appliance:

reset

[NOTE] Choose No when prompted to Save Config.

GUI Example: Restarting the SECURITY APPLIANCE

- System > Software
- Select the reboot button

4.6 ADDITIONAL SYSTEM MANAGEMENT TASKS

This section describes the additional system management options available through the <NetSecure 6100> management interface. This section includes the following topics:

- Viewing System Information
- Creating Aliases
- Deleting Aliases
- Viewing Current Aliases
- Configuring Domain Names
- Deleting Domain Names
- Configuring Host Names
- Deleting Host Names

4.6.1 VIEWING SYSTEM INFORMATION

You can use the **get system** command to display the following information about the <NetSecure 6100> hardware and firmware:

- Software Version
- System Uptime
- Vendor Name
- Vendor Contact
- Product Model
- Product Serial Number
- MAC Addresses

To view system information, use the **get system** command

get system
get system
++ system information

-- build version vf2112v2r1b17

-- build date ..... Tue May 16 18:29:03 UTC
2006
-- system uptime 01:03:22
++ manufacture information setting

-- vendor id 01
-- vendor name ..... <vendor>
-- vendor contact ..... <vendor>
-- manufacture code 00
-- manufacture date ..... 2006-02-28 12:21:00 UTC
-- product model ..... NetSecure 6100
-- product serial number 0001-02-0606-0074
-- ethernet 1 mac address 0:60:26:20:0:94
-- ethernet 2 mac address 0:60:26:20:0:95
-- hardware revision number .. 0:0
++ resources information

-- flash bootrom size ..... 0x2000000 bytes
-- flash jffs2 size ..... 0x2000000 bytes
-- ddr2-dram size ..... 0x40000000 bytes
-- tcam size ..... 18 Mbits
-- reset to default config ... none

-- running platform type .... security appliance
-- calibration frequency 38.4Mhz
-- running boot image ..... primary
-- running mos image ..... primary
-- total mos reboot count 1
-- mos last reboot date ..... 2006-05-22 16:58:07 UTC

++ post result

-- ddr2 memory test ..... passed
-- jffs2 flash memory test ... passed
-- test i2C bus ..... passed
-- test fan/temp controller... passed
-- test phy control dev ..... passed
-- test rtc device ..... passed
-- test external tcam ..... passed
-- test fiber ext-loopback ... passed

-- test copper ext-loopback .. passed

GUI Example: Viewing SYSTEM INFORMATION

System > Status

4.6.2 CREATING ALIASES

Use the **set alias** command to create an alias that is a named variable containing the initial characters of a command-line interface (CLI) command:

set alias {name_str} string

Example: Creating an ALIAS

To create an alias called int_0 for the get interface eth0, use the **set alias** command:

- set alias int_0 “get interface eth0”
- save

4.6.3 DELETING ALIASES

To remove an alias, use the **unset alias** command:

unset alias {name_str}

Example: Deleting an ALIAS

To remove a previously created alias called int_0:

unset alias int_0

4.6.4 VIEWING CURRENT ALIASES

To view a previously created alias, use the **get alias** command:

get alias

4.6.5 CONFIGURING DOMAIN NAMES

To configure the <NetSecure 6100> to respond to a specifically configured domain, use the **set domain** command:

set domain {name_str}

Example: Configuring the domain name MTAPPLIANCE

- set domain MTAPPLIANCE
- save

GUI Example: Configuring the domain name MTAPPLIANCE

- Network > DNS > add Domain Name
- Enter the following, then click **Apply**.
  Domain Name: MTAPPLIANCE

4.6.6 DELETING DOMAIN NAMES

To delete a previously configured domain name, use the **unset domain** command:

- unset domain
- save

4.6.7 CONFIGURING HOST NAMES

To configure a host name on the <NetSecure 6100> use the **set host** command:

set host {name_str}

Example: Confiuring the hose name MTTAPPLIANCE

- set host MTAppliance
- save

GUI Example: Confiuring the hose name MTTAPPLIANCE

- Network > DNS > add Host Name
- Enter the following, then click **Apply**.
  Host Name: MTAPPLIANCE

4.6.8 DELETING HOST NAMES

To delete a previously configured host name, use the **unset hostname** command:

unset host

4.7 USING NETWORK TIME PROTOCOL (NTP)

The <NetSecure 6100> uses Network Time Protocol (NTP) to update its internal date and time, and to include the date and time in its log messages. This protocol is required for any policies schedules. For additional information on schedules refer to Chapter 9 Policy Configuration.

This section describes how to use NTP with the <NetSecure 6100> in the following topics:

- Configuring NTP Settings
- Configuring the NTP Update Interval
- Viewing Current NTP Settings
- Deleting NTP Server IP Entries
- Configuring Manual Update using NTP
- Maintaining Clock Settings with NTP
- Configuring the Clock to Use NTP
- Configuring the Time Zone

4.7.1 CONFIGURING NTP SETTINGS

To configure the NTP settings used to update the date and time for the appliance, use the **set ntp server** command:

- set ntp server { ip_addr/dom_name}
- {primary|backup1|backup2}

Example: Setting the PRIMARY NTP server IP as 207.245.143.147

- set ntp server 207.245.143.147 primary
- save

GUI Example: Setting the PRIMARY NTP server IP as 207.245.143.147

- System > Date/Time
- Enter the following, then click **Apply**:
  Primary NTP Server IP/Name: 207.245.143.147

[NOTE] You can use a fully qualified domain name in place of an IP address.

4.7.2 CONFIGURING THE NTP UPDATE INTERVAL

The <NetSecure 6100> performs an NTP update at regular intervals to check the current date and time. The default NTP interval is 60 minutes. To configure the NTP update interval, use the **set ntp server** command.

set ntp interval {number}

The NTP interval is displayed in minutes.

Example: Changing the NTP update interval to 120:

- set ntp interval 120
- save

4.7.3 VIEWING CURRENT NTP SETTINGS

To view current NTP server settings, use the **get ntp** command:

get ntp

4.7.4 DELETING NTP SERVER IP ENTRIES

To delete an NTP server IP entry, use the **unset ntp server** command:

unset ntp server {ip_addr/dom_name}

Example: Deleting an NTP server entry using the IP address

207.245.143.147:

- unset ntp server 207.245.143.147
- save

GUI Example: Deleting an NTP server entry using the IP address 207.245.143.147:

- System > Date/Time
- Remove the following, then click **Apply**:
  Primary NTP Server IP/Name: 207.245.143.147

[NOTE] You can configure multiple NTP server IP addresses to ensure the <NetSecure 6100> always displays the correct date and time.

4.7.5 CONFIGURING MANUAL UPDATE USING NTP

To initiate a manual NTP update, use the **exec ntp** command:

exec ntp update

4.7.6 MAINTAINING CLOCK SETTINGS WITH NTP

Use the **set clock** command to ensure that the <NetSecure 6100> is configured with the correct date and time:

set clock {date [time] | dst-off | ntp | timezonenumber}

Use NTP for updates to the clock.

Example: Manually setting the CLOCK using 12/30/2004 12:00:

- set clock 12/30/2004 12:00
- save

4.7.7 CONFIGURING THE CLOCK TO USE NTP

To configure automatic updates to the clock through NTP, use the **set clock** command:

set clock ntp

4.7.8 CONFIGURING THE TIME ZONE

To configure the time zone setting for the clock, use the **set clock** command. The **timezone {number}** parameter represents the difference between your local time and standard Greenwich Mean Time. The number can be between -12 and 12. For instance, the Pacific Time zone is represented by -8.

set clock timezone {number}

Example: Confiuring the CLOCK TIME ZONE to PACIFIC TIME ZONE (GMT -8):

- set clock timezone –8
- save

GUI Example: Confiuring the CLOCK TIME ZONE to PACIFIC TIME ZONE (GMT -8):

- System > Date/Time
- Select the following, then click **Apply**:
  Set Time Zone: -8 hours

4.8 USING DOMAIN NAME SERVICE (DNS)

The Domain Name Service (DNS) host IP address allows the <NetSecure 6100> to resolve or match domain names to IP addresses. You must specify a DNS host in order to resolve domain names to IP addresses. Use the **set dns** command to configure one DNS host IP address for the appliance:

set dns host {host} {dns1|dns2}

You can configure additional DNS host IP addresses as necessary.

GUI Example: Confiuring the CLOCK TIME ZONE to PACIFIC TIME ZONE (GMT -8):

- set dns host dns1 206.13.31.12
- save

GUI Example: Setting the primary DNS host IP address as 206.13.31.12

- Interface > DNS
- Enter the following, then click **Apply**:
  Primary DNS Server IP Address: 206.13.31.12

Example: Setting a secondary DNS host IP address as 206.13.28.12:

- set dns host dns2 206.13.28.12
- save

GUI Example: Setting a secondary DNS host IP address as 206.13.28.12:

- Interface > DNS
- Enter the following, then click **Apply**:
  Secondary DNS Server IP Address: 206.13.28.12

4.8.1 DELETING DNS HOST IP ADDRESSES

To delete a DNS host IP address, use the **unset dns** command:

unset dns {host} {dns1|dns2}

Example: Deleting the secondary DNS host IP address 206.13.28.12

- unset dns2
- save

GUI Example: Deleting the secondary DNS host IP address 206.13.28.12

- Interface > DNS
- Delete the following, then click **Apply**:
  Secondary DNS Server IP Address: 206.13.28.12

4.8.2 DISPLAYING CURRENT DNS HOST SETTINGS

To display the current DNS host IP settings, use the **get dns** command:

- get dns host settings

4.9 USING PING

To test connectivity to other hosts connected to the <NetSecure 6100> for Internet connectivity, use the **ping** command:

ping {ip_addr|dom_name}

EXAMPLE: PING WWW.YAHOO.COM

ping www.yahoo.com

GUI EXAMPLE: PING WWW.YAHOO.COM

- System > Tools
- Enter the following, then click **Apply**:
  Diagnostic Tool: Ping
  Ping: www.yahoo.com

4.10 USING TRACEROUTE

You can use traceroute to trace packets from your machine to an Internet host, showing you the number of hops and time required to reach the host along the path. To execute the **trace-route** command:

- trace-route {ip_addr|dom_name }

Example: TRACEROUTE www.yahoo.com:

- trace-route www.yahoo.com

GUI Example: TRACEROUTE www.yahoo.com:

- System > Tools
- Enter the following, then click **Apply**:
  Diagnostic Tool: Traceroute
  Traceroute: www.yahoo.com

Chapter 5. Attack Detection & Prevention

This chapter describes different types of denial of service (DoS) and distributed denial of service (DDoS) attacks that can affect the <NetSecure 6100>. It also describes how you can prevent such attacks and how to configure attack prevention options. This chapter includes the following topics:

- Network Attacks
- Attack Stages
- Detecting an Attack
- Preventing Network Port Attacks
- About Denial of Service (DoS and DDoS) Attacks
- Preventing Network Port Attacks
- Additional Attack Detection and Prevention
- Viewing Attack Settings

5.1 NETWORK ATTACKS

Attackers invade a protected network for any of the following reasons:

- To gather information about the hosts on the protected network, including details about:
  - Topology of the network.
  - Number of active hosts on the network.
  - Different services or ports available on an active host.
  - Type of operating system on the active machines.

- To try to overwhelm the network with bogus traffic to induce a denial of service.
- To cause damage to or steal data from a protected host.
- To gain access to a protected host to steal confidential information.
- To gain access to a protected host to launch additional attacks.
- To gain control of the firewall access control list.

5.2 ATTACK STAGES

Attacks usually happen in two steps:

- The attacker gathers information by:
  - Performing an IP address sweep to determine which hosts on the network are active.
  - Determining the active ports on host found during the IP address sweep.
  - Determining the current operating system of the host and weaknesses in that operating system.
- The attacker launches the attack by:
  - Concealing the attack.
  - Executing the attack.
  - Removing or hiding evidence of the attack.

5.3 DETECTING AN ATTACK

To prevent hackers from exploiting a network, the appliance uses stateful inspection to dynamically filter and secure all network connections. Stateful inspection enables the appliance to note components in the IP packet and TCP segment headers, including the source and destination IP addresses, source and destination ports and packet sequence numbers. This information maintains the state of each TCP session and UDP session traversing a security policy. When a responding TCP packet arrives, the appliance compares the information in the header with the state entries currently in the state table. If the appliance finds a match, it allows the responding packet to pass through the firewall. If the appliance does not find a match, it drops or rejects the packet.

Table 5-1 lists the range of network and operating system-specific attacks that the security appliance can detect and defend against.

Table 5-1 Network and Operating System –Specific Attacks

Attack Name	Description
Back Orifice Attack	Occurs when a hacker attempts to drop a Trojan horse communicating over port 31337 onto a remote computer. If the attempt is successful, a hacker can take screen captures, execute keyboard commands, make file transfers and install applications on the victim computer.
Inikiller Attack	Communicates over port 9989 and allows an attacker to destroy .ini files on remote workstations.
IP Spoof	An attacker forms and sends messages to a computer, as if they were communicating on the same trusted network. A hacker enlists a number of techniques to find a trusted host, modify the IP header information and attempt to spoof.
ICMP Router Discovery Protocol (IRDP)	An attacker supersedes the default route for the host by inserting a more specific route. Once the new route is added, an attacker can forward all traffic from the host in order to gather information, launch a man-in-the-middle attack or create a DoS by adding or restoring default routes.

Attack Name	Description
Netbus Attack	Affects Windows 95, 98 and NT operating systems. A netbus attack allows hackers to install a Trojan horse that enables them to open and close CD-ROM drives, start applications and redirect URLs.
NetSpy Attack	Hackers install a Trojan horse enabling control of a remote system via port 1024.
Senna Spy Attack	A Trojan horse attack that allows the hacker to take control of a remote workstation via port 13000. Allows the attacker to perform illicit activity on that machine.
Striker Attack	Form of a Trojan horse attack that allows a hacker to crash a system over port 2565.
Sub Seven Attack:	Attackers send a Trojan horse over ports 6667, 6711 and 27374. Allows the hacker to perform illicit activities on the remote machine. This attack is particularly dangerous because IRC messages can be sent back to the hacker letting them know if the system is up or down.
Port Scan	A hacker sends requests to all ports, one at a time, to determine whether the port is in use by a system. This allows the hacker to take advantage of weaknesses in a specific system. Port scanning is used by hackers to gather information about a specific network or range of IP addresses.
Priority Attack	A hacker communicates over port 16969. The hacker drops a Trojan horse to enable illicit activity on a remote machine.

5.4 ABOUT DENIAL OF SERVICE (DOS AND DDOS) ATTACKS

Not all attacks attempt to gain unauthorized access into a protected network. Some attacks attempt to hinder normal network activity by sending large amounts of bogus data consuming all of the resources on that host or hosts. These attacks are called denial of service (DoS) or distributed denial of service (DDoS) attacks. Table 5-2 lists these attacks.

Table 5-2 DoS and DdoS Attacks

Attack Name	Description
Smurf Attack	Swamps an Internet connection with many ICMP reply messages. The attack happens when a hacker sends an ICMP request to an Internet Broadcast address causing all of the machines on that network to reply. Since the IP address is likely a spoofed one, access to the Internet for t he machine is cut off.
Fraggle Attack	Very similar to a smurf attack, but performed over UDP instead of ICMP.
Land Attack	An attacker sends a packet with the same source and destination information as another machine on a network. This causes the real machine on the network to think that it sent the packet to itself, causing a resource slowdown.
SYN-Flood	Uses packets that have an unreachable source address to establish a large number of connections. This type of attack exhausts all resources available on a network device so it no longer processes valid requests.
Ping of Death	Sends a large IP packet request that is larger than 65,536. Since IP allows fragmentation, an attacker could send multiple IP packets that, when assembled, are larger than 65,536. This causes systems to crash or freeze.
Teardrop Attack	An attacker sends a large data packet in need of fragmentation. This fragmentation enables the attacker to set an offset at the beginning of the packet, allowing the end machine to reassemble the large packet. During reassembly, the hacker uses a confusing offset that might crash the

Attack Name	Description
	receiving machine or cause it to go offline.
UDP Bomb	Enable hackers to craft packets with illegal values in certain fields. If these packets reach older machines, these illegal packets might crash the machine.
WinNuke	A DoS attack targeted at machines running Windows. Using the NetBIOS port 139, an attacker sends a TCP packet with an urgent (URG) flag to a host with an established connection, causing the Windows machine to crash.

5.5 PREVENTING NETWORK PORT ATTACKS

Using the global zone, you can configure the security appliance with additional port attack prevention that will be enabled or disabled on the global zone. Use the **set policy** command to enable detection and prevention of network port attacks:

set policy global port-attacks {attack_str}

You can use the following specific port attacks in the set policy command:

- All
- Back-orifice
- Ini-killer
- Netbus
- Netspy
- Priority
- Ripper
- Senna-spy
- Small-server
- Seb-seven
- Striker

[NOTE] In addition, you set the **global port-attack** option to *all* to prevent all attacks listed above. Alternatively, you can set the **global port-attack** option to *none* to disable attack prevention.

Example: Preventing network port attacks

To enable all network port attack detection and prevention for the global zone:

- set policy global port-attack all

- save

GUI Example: Preventing network port attacks

- Policy > Attack Configuration: Global
- Select the following, then click **Apply**:
  Check All

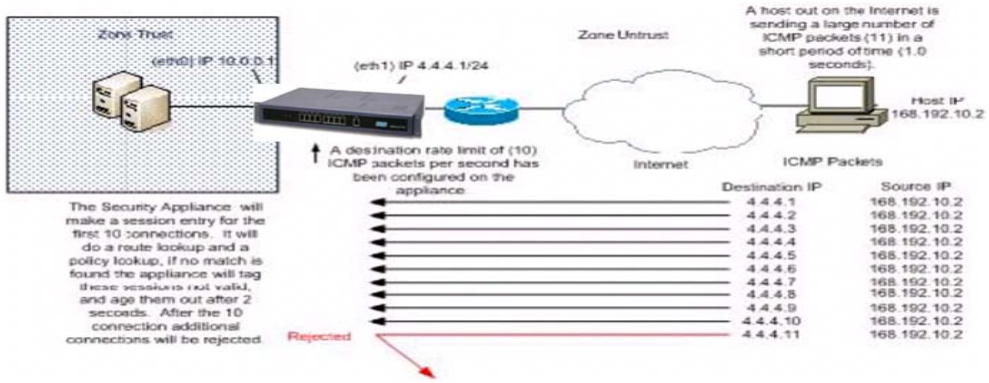
To unset port attacks, use the **unset policy global** command

- unset policy global port attack {attack_str}
- save

5.6 CONFIGURING THE < NetSecure 6100> TO DEFEND AGAINST DOS AND DDOS ATTACKS

Rate limiting is the most common method to defend against DoS and DDoS attacks (refer to Figure 5-1 for an example of a DoS attack). You can configure options on the appliance to apply various rate limits to ICMP, TCP, and UDP traffic.

Figure 5-1 Example of a DoS Attack


Zone Trust
(eth0) IP 10.0.0.1
(eth1) IP 4.4.4.1/24
Zone Untrust
A host out on the Internet is sending a large number of ICMP packets (11) in a short period of time (1.0 seconds).
Host IP
168.192.10.2
A destination rate limit of (10) ICMP packets per second has been configured on the appliance
Internet
ICMP Packets
The Security Appliance will make a session entry for the first 10 connections. It will do a route lookup and a policy lookup, if no match is found the appliance will tag these sessions not valid, and age them out after 2 seconds. After the 10 connection additional connections will be rejected
Rejected
Destination IP
Source IP
4.4.4.1
4.4.4.2
4.4.4.3
4.4.4.4
4.4.4.5
4.4.4.6
4.4.4.7
4.4.4.8
4.4.4.9
4.4.4.10
4.4.4.11
168.192.10.2

Rate limiting is a function in which a network interface limits the number of packets sent or received allowing traffic that is less than or equal to the rate to be sent. For any traffic that exceeds the limit, the network interface might drop or delay it. The security appliance uses policy control to limit the amount of traffic on a specified interface. If traffic exceeds the rate that the administrator sets, the security appliances drops additional packets.

5.6.1 CONFIGURING ICMP FLOOD PREVENTION

To configure the rate limit for ICMP traffic for a specific zone, use the **set zone** command with the **icmp-flood attack-threshold** option. This enables you to set limits (per second) on the number of ICMP packets allowed through that zone to a specific host.

set zone {zone name} screen icmp-flood attack-threshold {number}

Example: Setting the ICMP threshold

Set the ICMP threshold to 1,000 on the untrust zone:

- set zone untrust screen icmp-flood attack-threshold 1000
- save

GUI Example: Setting the ICMP threshold

- Policy > Attack Settings Edit Zone (for “unturst”)
- Enter the following, then click **Apply**:
  ICMP flood attack threshold: 1000

5.6.2 CONFIGURING UDP FLOOD PREVENTION

To configure the rate limit for UDP datagrams in a specific zone, use the **set zone** command with the **udp-flood attack-threshold** option:

set zone {zone name} screen udp-flood attack-threshold {number}

This sets a rate limit for the number of UDP datagrams allowed through the zone to a specific host per second. The maximum threshold for the **udp-flood attack-threshold** is 64,000.

5.6.3 CONFIGURING SYN FLOOD PREVENTION

A host or multiple hosts that sends a large number of invalid SYN packets can overwhelm network devices. This causes network devices to allocate more resources to process the invalid SYN requests, leaving fewer resources available to process legitimate traffic requests. If you apply rate limits to restrict the number of SYN packets allowed through a zone, the appliance detects and protects against SYN flood attacks.

Use the **set zone** command with the **syn-flood attack threshold** option to set a limit on the number of SYN packets that a specific zone can receive per second before being dropped:

set zone {zone name} screen syn-flood attack-threshold {number}

Example: Setting the SYN flood threshold

Set the SYN flood attack threshold to 5,000 on the untrust zone:

- set zone untrust screen syn-flood attack-threshold 5000
- save

GUI Example: Setting the SYN flood threshold

- Policy > Attack Settings Edit Zone (for “untrust”)
- Enter the following, then click **Apply**:
  SYN flood attack threshold: 5000

5.6.4 CONFIGURING FIN FLOOD PREVENTION

Setting a rate limit for FIN packets allows the appliance to detect and prevent FIN flood attacks. Use the **set zone** command with the **fin-flood attack threshold** option to limit the number of FIN packets that a specific zone can receive per second before being dropped:

set zone {zone name} screen fin-flood attack-threshold {number}

Example: Setting the FIN flood threshold

Set the FIN flood threshold to 2,000 on the untrust zone:

- set zone untrust screen fin-flood attack-threshold 2000
- save

GUI Example: Setting the FIN flood threshold

- 1Policy > Attack Settings Edit Zone (for “untrust”)
- Enter the following, then click **Apply**:
  FIN flood attack threshold: 2000

5.6.5 CONFIGURING IP FRAGMENT PREVENTION

To limit the number of fragmented IP packets a specific interface can receive per second, use the **set zone** command with the **ip-frag attack-threshold** option:

set zone {zone name} screen ip-frag attack-threshold {number}

Example: Setting the IP fragment threshold

Set the ip-frag threshold to 1,000 on the untrust zone:

- set zone untrust screen ip-frag attack-threshold 1000
- save

GUI Example: Setting the IP fragment threshold

- Policy > Attack Settings Edit Zone (for “untrust”)
- Enter the following, then click **Apply**:
  IP-frag attack threshold: 1000

5.6.6 CONFIGURING TCP-FIN-NO-ACK

To filter packets that have a TCP-FIN bit set, but no ACK, use the **set zone** command:

set zone {zone name} screen fin-no-ack

Example: Configuring TCP-FIN-no ack

To filter packets that have a TCP-FIN bit set, but no ACK for the untrust zone:

- set zone untrust screen fin-no-ack
- save

GUI Example: Configuring TCP-FIN-no ack

- Policy > Attack Settings Edit Zone (for “untrust”)

- Select the following, then click **Apply**:
  Screen FIN-no-ACK

5.7 ADDITIONAL ATTACK DETECTION AND PREVENTION

In addition to the configurable attack settings the appliance detects and prevents the following network and DoS attacks:

- Land Attack
- TCP-SYN-and-FIN flags set
- IP spoof
- IRDP
- Teardrop attack
- TCP-no flags set
- Ping of Death
- Smurf attack
- TCP-no flags set
- Unknown IP protocol
- UDP bomb

5.8 VIEWING ATTACK SETTINGS

To view the current attack settings per zone, use the **get zone** command with the **screen** and zone name to view the current settings:

get zone {zone name} screen

Example: Viewing attacks setting on untrust zone

- cli-> get zone untrust screen
- ID: 2
- Type: Pre-defined
- Zone: untrust
- Intra-zone block: Off
- Flags: IcmpFrag IcmpLarge FinNoAck
- SynFlood: 65535
- FinFlood: 65535
- cmpFlood: 16777215
- FragFlood: 16777215

GUI Example: Viewing attacks setting on untrust zone

- Network > Zone Edit (for “untrust”)
- Select the following, then click **Apply**:
  Screen

Chapter 6. Logging

This Chapter describes the options available for event logging, storing and receiving logs and Simple Network Management Protocol (SNMP).

- Logging
- Logging Levels
- Log Modules
- Traffic and Event Log Management
- Log Module Settings
- Admin Mail Server
- Syslog Management
- SNMP MIB Groups
- Configuring SNMP on the NetSecure 6100

6.1 LOGGING

Logging is the process of recording and storing information about a specific event. On the security appliance a single activity that occurs, such as denying a packet from passing through a zone is considered an individual event. Since the security appliance will be used to protect network infrastructures it becomes extremely important to record all events showing a possible security problem. Logging is an important part of an effective network security policy. For example, an increased number of denied packets from the same source can show an unauthorized person tried to access your network. You can configure your firewall to log a variety of events, including denied packets, network attacks and IKE information.

6.2 LOGGING LEVELS

The security appliance provides many different log messages related to the operation of the appliance including administration configuration changes, self generating messages and alarms regarding the operational behavior and attacks. The security appliance uses the categories listed below to categorize the different events:

- **Information Messages**—Information messages regarding the general operation of the security appliance.
- **Notification Messages**—Messages related to normal events, including administration changes.
- **Warning Messages**—Events that could affect the functionality of the security appliance.
- **Error Messages**—Messages that include error conditions that may exist on the security appliance.
- **Critical Messages**—Events that could affect functionality of the security appliance.
- **Alert Messages**—Events that require immediate attention by you that include attacks against the security appliance.
- **Emergency Messages**—Messages that may need immediate attention by the administrator.
- **Debug Messages**—Message information used to diagnose or troubleshooting specific issues with the security appliance.

6.3 LOG MODULES

To allow for more flexible log management each of the different software components can have a unique log setting. The software modules are as follows:

- ARP
- CFG
- Log
- Upset
- NAT
- Session
- Policy
- Route
- RIP
- SNMP
- DoS
- IP
- RIP
- FUB
- SRMMGR

6.4 TRAFFIC AND EVENT LOG MANAGEMENT

To get log information from the security appliance at least one destination must be specified. Log destinations include:

- Console
- Internal
- E-mail
- Syslog
- SSH

6.5 LOG MODULE SETTINGS

6.5.1 SETTING LOG MODULES

To enable logging for a specific software module use the **set log module** command with the software module option, the desired logging level and message destination.

set log module {module} level {all| informational|
notification| warning| error| critical| alert|
emergency| debug} destination {console| internal| email|
syslog| ssh}

Example: Set the log module for ARP using the log level all with a destination of the console.

- set log module arp level all destination console
- save

GUI Example: Set the log module for ARP using the log level all with a destination of the console.

Logging > Log Settings: Select the following, then click **Apply**:
Module: arp
Destination Console: All

6.5.2 DISABLING LOG MODULE SETTINGS

To disable the software module settings use the unset log module command.

unset log module {module} level {all| informational|
notification| warning| error| critical| alert|
emergency| debug} destination {console| internal| email|
syslog| ssh}

6.5.3 VIEWING THE LOG MODULE SETTINGS

To view the log module settings use the **get log settings** command.

get log setting Levels:

0=Emergency,
1=Alert,
2=Critical,
3=Error,
4=Warning,
5=Notification,
6=Information,
7=Debugging,
8=Tracing
'-'=disabled

Module	Console	Internal	Email	Syslog	Current-SSH
interface	----------	----------	----------	----------	----------
service	----------	----------	----------	----------	----------
ike	----------	----------	----------	----------	----------
policy	----------	----------	----------	----------	----------
route	----------	----------	----------	----------	----------
arp	012345678	----------	----------	----------	----------
cfg	----------	----------	----------	----------	----------
log	----------	----------	----------	----------	----------
rip	----------	----------	----------	----------	----------
rib	----------	----------	----------	----------	----------
fup	----------	----------	----------	----------	----------
snmp	----------	----------	----------	----------	----------
srmmgr	----------	----------	----------	----------	----------

6.5.4 VIEWING THE TRAFFIC AND EVENT LOG

The security appliance has maximum storage of 2Mb for event logging. In the event that the 2Mb limit is reached the security appliance will over write the oldest event logs and replace them with newer events. All messages logged will include date and time. To view the event log you will use the **get log messages** command to show the event logs to show all events logged.

```
cli-> get log message

Jun 09 20:28:58 2006 vendor name id=security_appliance
policy[117] [INFO] id=1 proto=1 src=64.62.250.2:0
dst=64.79.127.67:0 packet dropped due to policy deny!

Jun 09 20:29:05 2006 vendor name id=security_appliance
policy[117] [INFO] id=1 proto=1 src=64.62.250.2:0
dst=64.79.127.67:0 packet dropped due to policy deny!

Jun 09 20:29:11 2006 vendor name id=security_appliance
policy[117] [INFO] id=1 proto=1 src=64.62.250.2:0
dst=64.79.127.67:0 packet dropped due to policy deny!

Jun 09 20:29:16 2006 vendor name id=security_appliance
policy[117] [INFO] id=1 proto=1 src=64.62.250.2:0
dst=64.79.127.67:0 packet dropped due to policy deny!

cli->
```

[NOTE]: The event logs stored local to the security appliance will be erased if the appliance is powered down or rebooted. You should configure a syslog server to collect all logs.

GUI Example: View the traffic and event logs

- Reports > System Log > Events
- Shows the current log messages stored in the flash

6.6 ADMIN MAIL SERVER

6.6.1 CONFIGURE THE SECURITY APPLIANCE TO SEND E-MAIL NOTIFICATION USING THE ADMIN MAIL OPTION

E-mail message notification can be configured allowing the security appliance to send e-mail messages. Using the **set admin** command with the **mail** option will allow configuration of the mail server IP address or name and the administrators e-mail addresses.

- set admin mail server-name {ip_addr/name}
- set admin mail {mail-addr1/mail-addr2} {e-mail_addr}

Example: Sending e-mail message to the administrator of the SECURITY APPLIANCE using the SMTP server IP 10.0.0.5 and the e-mail adress admin@yourcompany.com

- Mail server: 10.0.0.5
- Recipient address1: admin@yourcompany.com
- save

GUI Example: Sending e-mail message to the administrator of the SECURITY APPLIANCE using the SMTP server IP 10.0.0.5 and the e-mail adress admin@yourcompany.com

- Logging > SMTP
- Enter the following, then click Apply:
  System Name: admin
  System Contact: admin@yourcompany.com
  Location: 10.0.0.5

6.6.2 DELETING THE ADMIN MAIL SERVER

To delete the e-mail messages settings use the **unset admin mail** command with the **server-name** option.

unset admin mail server-name

6.6.3 REMOVING E-MAIL ADDRESSES FROM THE ADMIN MAIL SERVER

To remove an e-mail address so messages are no longer sent to that e-mail address use the **unset admin mail** address with the **mail-addr1| mail-addr2** option.

unset admin mail mail-addr1

6.7 SYSLOG MANAGEMENT

The security appliance can generate syslog messages specified for delivery to multiple syslog servers. The syslog protocol uses a standard transport mechanism along with a standard format for all messages. This allows multiple network devices to send syslog information that can formatted into custom reports. Up to three syslog servers can be specified using the **set syslog** command.

- set syslog config {ip_address}
- set syslog config {ip_address} log {all |event |traffic}
  set syslog config {ip_address} facilities {local0 |local1 |local2 |local3 |local4 |local5 |local6 |local7}
- set syslog config {ip_address} port {port_number}

Example: Configure both traffice and event message to be sent using SYSLOG to a server at IP address 10.0.0.200 with the facility of Local0

- set syslog config 10.0.0.200
- set syslog config 10.0.0.200 log all
- set syslog config 10.0.0.200 facilities local0
- save

GUI Example: Configure both traffice and event message to be sent using SYSLOG to a server at IP address 10.0.0.200 with the facility of Local0

- Logging > Syslog Settings 2 Enter the following, then click **Appl**y:
  Enable Syslog Messages
  IP/Host Name: 10.0.0.200
  Facility: local0
  Event Log
  Traffic Log

6.7.1 DELETING THE SYSLOG HOST IP ADDRESS

To delete the syslog host IP address use the **unset syslog config** command with the **IP** option.

unset syslog config ip

6.7.2 DISABLING THE SYSLOG HOST LOG OPTIONS

To disable the syslog host log option use the **unset syslog config ip log** and specify the current log option to disable.

unset syslog config ip log {all| traffic| event}

6.7.3 SYSLOG MESSAGE FORMAT

When the security appliance generates and sends syslog messages for delivery to the syslog server, the format for the messages is standard.

6.7.4 SYSLOG MESSAGE SAMPLE:

- 192.168.65.230: <134>Jun 02 12:13:54 2006 vendor name
- id=security_appliance policy[117] [INFO]
- id=1
- proto=1
- src=64.62.250.2:0
- dst=64.79.127.67:0 packet dropped due to policy deny

Table 6-1 shows the syslog message format.

Table 6-1 Syslog Message Format

Field Example	Field Name	Description
Jun 02	Month and Day Stamp	Displays the month and day when the message was generated.
12:13:54	Time stamp	Displays the time stamp when the message was generated. The format is as follows HH:MM:SS.
2006	Year Stamp	Displays the year when the message was generated.
Vendor name	Device name	Displays the vendor name.
Security_Appliance	Device id	Displays the hostname for the appliance.
Policy	Software module name	Displays the software module name that generated the log message.
[117]	Software module process ID	Displays the software module process ID that generated the log message.
INFO	Log level	Displays the log severity level.
ID=1	Device ID	Displays the ID number of the device.
Proto=1	Protocol number	Displays the protocol or service number.
src=64.62.250.2:0	Source IP address and port number	Displays the source IP address and port number of the packet.
dst=64.79.127.67:0	Destination IP address and port number	Displays the destination IP address and port number of the packet.
packet dropped due to policy deny	Message txt	Displays the log message.

6.8 SNMP MIB GROUPS

Simple Network Management protocol (SNMP) is a protocol used by network management systems for monitoring network attached devices for conditions that warrant administrator attention.

The SNMP agent that resides on the security appliance will allow for SNMP v1 and 2c get functionality. The following Management Information Base (MIB) groups are supported:

- System group (.1.3.6.1.2.1.1) (RFC 1213)
- Interface group (.1.3.6.1.2.1.2) (RFC 2233)
- Address Translation group (.1.3.6.1.2.1.3)
- IP group (.1.3.6.1.2.1.4) (RFC 2011)
- ICMP group (.1.3.6.1.2.1.5) (RFC 1213)
- TCP group (.1.3.6.1.2.1.6) (RFC 2012)
- UDP group (.1.3.6.1.2.1.7) (RFC 2013)
- Transmission group (Ethernet) (.1.3.6.1.2.1.10) (RFC 1643)
- SNMP group (1.3.6.1.2.1.11) (RFC 1213)

6.8.1 SYSTEM GROUP

Table 6-2 shows the System Group

Table 6-2 System Group

Object Name	Value Type
sysDescr	DisplayString
sysObjectID	OBJECT ID
sysUpTime	TimeTicks
sysContact	DisplayString
sysName	DisplayString

Object Name	Value Type
sysLocation	DisplayString

6.8.2 INTERFACE GROUP

Table 6-3 shows the Interface Group

Table 6-3 Interface Group

Object Name	Value Type
ifNumber	Integer32
ifTableLastChange	TimeTicks

6.8.3 ADDRESS TRANSLATION GROUP

Table 6-4 shows the Address Translation Group

Table 6-4 Address Translation Group

Object Name	Value Type
atIfIndex	INTEGER,
atPhysAddress	PhysAddress,
atNetAddress	NetworkAddress

6.8.4 IP GROUP

Table 6-5 shows the IP Group

Table 6-5 IP Group

Object Name	Value Type
ipForwarding	INTEGER
ipDefaultTTL	INTEGER
ipInReceives	Counter32
ipInHdrErrors	Counter32
ipInAddrErrors	Counter32

Object Name	Value Type
ipForwDatagrams	Counter32
ipInUnknownProtos	Counter32
ipInDiscards	Counter32
ipInDelivers	Counter32
ipOutRequests	Counter32
ipOutDiscards	Counter32
ipOutNoRoutes	Counter32
ipReasmTimeout	Counter32
ipReasmReqds	Counter32
ipReasmOKs	Counter32
ipReasmFails	Counter32
ipFragOKs	Counter32
ipFragFails	Counter32
ipFragCreates	Counter32

6.8.5 IP ADDRESS

Table 6-6 shows the IP Address Table

Table 6-6 IP Address Table

Object Name	Value Type
ipAdEntIfIndex	INTEGER
ipAdEntNetMask	IpAddress
ipAdEntBcastAddr	INTEGER
ipAdEntReasmMaxSize	INTEGER

6.8.6 IP ROUTE

Table 6-7 shows the IP Route Table

Table 6-7 IP Route Table

Object Name	Value Type
ipRouteDest	IpAddress
ipRouteIfIndex	INTEGER
ipRouteMetric1	INTEGER
ipRouteMetric2	INTEGER
ipRouteMetric3	INTEGER
ipRouteMetric4	INTEGER
ipRouteNextHop	IpAddress
ipRouteType	INTEGER
ipRouteProto	INTEGER
ipRouteAge	INTEGER
ipRouteMask	IpAddress
ipRouteMetric5	INTEGER
ipRouteInfo	OBJECT ID

6.8.7 IP NET TO MEDIA

Table 6-8 shows the IP Net to Media Table

Table 6-8 IP Net to Media Table

Object Name	Value Type
ipNetToMediaIfIndex	INTEGER
ipNetToMediaPhysAddress	PhysAddress
ipNetToMediaNetAddress	IpAddress
ipNetToMediaType	INTEGER

6.8.8 ICMP GROUP SCALARS

Table 6-9 shows the ICMP Group Scalars Table

Table 6-9 ICMP Group Scalars

Object Name	Value Type
icmpInMsgs	Counter32
icmpInErrors	Counter32
icmpInDestUnreachs	Counter32
icmpInTimeExcds	Counter32
icmpInParmProbs	Counter32
icmpInSrcQuenchs	Counter32
icmpInRedirects	Counter32
icmpInEchos	Counter32
icmpInEchoReps	Counter32
icmpInTimestamps	Counter32
icmpInTimestampReps	Counter32
icmpInAddrMasks	Counter32
icmpInAddrMaskReps	Counter32
icmpOutMsgs	Counter32
icmpOutErrors	Counter32
icmpOutDestUnreachs	Counter32
icmpOutTimeExcds	Counter32
icmpOutParmProbs	Counter32
icmpOutSrcQuenchs	Counter32
icmpOutRedirects	Counter32
icmpOutEchos	Counter32
icmpOutEchoReps	Counter32
icmpOutTimestamps	Counter32
icmpOutTimestampReps	Counter32
icmpOutAddrMasks	Counter32
icmpOutAddrMaskReps	Counter32

6.8.9 TCP GROUP SCALARS

Table 6-10 shows the TCP Group Scalars Table

Table 6-10 ICMP Group Scalars

Object Name	Value Type
tcpRtoAlgorithm	INTEGER
tcpRtoMin	Integer32
tcpRtoMax	Integer32
tcpMaxConn	Integer32
tcpActiveOpens	Counter32
tcpPassiveOpens	Counter32
tcpAttemptFails	Counter32
tcpEstabResets	Counter32
tcpCurrEstab	Counter32
tcpInSegs	Counter32
tcpOutSegs	Counter32
tcpRetransSegs	Counter32
tcpInErrs	Counter32
tcpOutRsts	Counter32

6.8.10 TCP CONNECTION

Table 6-11 shows the TCP Connection Table

Table 6-11 TCP Connection Table

Object Name	Value Type
tcpConnState	INTEGER
tcpConnLocalAddress	IpAddress
tcpConnLocalPort	INTEGER
tcpConnRemAddress	IpAddress
tcpConnRemPort	INTEGER

6.8.11 UDP GROUP SCALARS

Table 6-12 shows the UDP Scalars Table

Table 6-12 UDP Scalars Table

Object Name	Value Type
udpInDatagrams	Counter32
udpNoPorts	Counter32
udpInErrors	Counter32
udpOutDatagrams	Counter32

6.8.12 UDP LISTENER

Table 6-13 shows the UDP Listener Table

Table 6-13 UDP Listener Table

Object Name	Value Type
udpLocalAddress	IpAddress
udpLocalPort	INTEGER

6.8.13 SNMP GROUP

Table 6-14 shows the SNMP Group Table

Table 6-14 SNMP Group Table

Object Name	Value Type
snmpInPkts	Counter32
snmpOutPkts	Counter32
snmpInBadVersions	Counter32
snmpInBadCommunityNames	Counter32
snmpInBadCommunityUses	Counter32
snmpInASNParseErrs	Counter32
snmpInTooBigs	Counter32

Object Name	Value Type
snmpInNoSuchNames	Counter32
snmpInBadValues	Counter32
snmpInReadOnlys	Counter32
snmpInGenErrs	Counter32
snmpInTotalReqVars	Counter32
snmpInTotalSetVars	Counter32
snmpInGetRequests	Counter32
snmpInGetNexts	Counter32
snmpInSetRequests	Counter32
snmpInGetResponses	Counter32
snmpInTraps	Counter32
snmpOutTooBigs	Counter32
snmpOutNoSuchNames	Counter32
snmpOutBadValues	Counter32
snmpOutGenErrs	Counter32
snmpOutGetRequests	Counter32
snmpOutGetNexts	Counter32
snmpOutSetRequests	Counter32
snmpOutGetResponses	Counter32
snmpOutTraps	Counter32
snmpEnableAuthenTraps	INTEGER
snmpSilentDrops	Counter32
snmpProxyDrops	Counter32

6.8.14 TRANSMISSION GROUP (DOT3STATS)

Table 6-15 shows the Transmission Group (DOT3STATS Table)

Table 6-15Transmission Group (DOT3STATS Table)

Object Name	Value Type
dot3StatsIndex	INTEGER
dot3StatsAlignmentErrors	Counter32
dot3StatsFCSErrors	Counter32
dot3StatsSingleCollisionFrames	Counter32
dot3StatsMultipleCollisionFrames	Counter32

dot3StatsSQETestErrors	Counter32
dot3StatsDeferredTransmissions	Counter32
dot3StatsLateCollisions	Counter32
dot3StatsExcessiveCollisions	Counter32
dot3StatsInternalMacTransmitErrors	Counter32
dot3StatsCarrierSenseErrors	Counter32
dot3StatsIndex	INTEGER
dot3StatsAlignmentErrors	Counter32

6.8.15 TRANSMISSION GROUP (DOT3COLLISION)

Table 6-16 shows the Transmission Group (DOT3COLLISION Table)

Table 6-16 Transmission Group (DOT3COLLISION Table)

Object Name	Value Type
dot3CollCount	Counter32
dot3CollFrequencies	Counter32

6.9 CONFIGURING SNMP ON THE SECURITY APPLIANCE

The following SNMP attributes can be configured on the security appliance. They include:

- **Community String—**Allows the SNMP community string and host to be set on the security appliance.
- **UDP Listening Port—S**ets the SNMP listening port on the security appliance.
- **System Name—**Allows the administrator to set the SNMP system name.
- **System Location**—Sets the security appliance system location.
- **System Contact—**Sets the SNMP system contact.

GUI Example: Configure SNMP settings

- **Logging > SNMP**
- Enter the following SNMP settings and click **Apply**:
  Type System Name: NetSecure 6100
  Type System Contact: Jon Smith
  Type System Location: Lab
  Type Listen Port: 161
  Type Trap Host : 162
- **SNMP > Community >Edi**t
- Enter the following SNMP Community settings and click Apply :
  Type Name: public
  Type Host: 192.168.1.1

6.9.1 ENABLING SNMP ON A SPECIFIED INTERFACE

To allow the SNMP monitoring system to contact and pull the SNMP information from the security appliance, SNMP must be enabled on that specified interface.

set interface {interface name} manage snmp

Example: To enable SNMP on theETH0 interface

set interface eth0 manage snmp

GUI Example: To enable SNMP on theETH0 interface

- Network > Interface > Edit (for ethernet0)
- Enter the following, then click Apply.
  Manage option: SNMP

Example: To disable SNMP on the ETH0 interface

unset interface eth0 manage snmp

GUI To disable SNMP on the ETH0 interface

- Network > Interface > Edit (for ethernet0)
- Enter the following, then click **Apply**.
  Manage option: Uncheck SNMP

6.9.2 CONFIGURING THE SNMP COMMUNITY STRING

To configure the SNMP community string use the **set snmp community** command. This will allow the community string and the host IP address to be entered.

set snmp community {string} host {host| OID}

6.9.3 CONFIGURING THE SNMP LISTENER PORT

To configure the SNMP listener port use the **set snmp port** command and specify the SNMP listener port the security appliance listen on.

set snmp port {port}

[NOTE] The default SNMP listener port is 161.

6.9.4 CONFIGURING THE SNMP SYSTEM NAME

To configure the SNMP system name use the **set snmp name** command and specify the name to be used as the system name.

set snmp name {name_str}

6.9.5 DELETING THE SNMP SYSTEM NAME

To delete the SNMP system name use the **unset snmp name** command.

unset snmp name

6.9.6 CONFIGURING THE SNMP SYSTEM LOCATIONS

To configure the SNMP system location use the **set snmp location** command and specify the physical location of the security appliance.

set snmp location {location}

6.9.7 DELETING THE SNMP LOCATION

To delete the SNMP location, use the **unset snmp location** command.

unset snmp location

6.9.8 CONFIGURING THE SNMP SYSTEM CONTACT

To configure the SNMP system contact use the **set snmp contact** command and specify the security appliance system contact.

set snmp contact {contact_str}

6.9.9 DELETING THE SNMP SYSTEM CONTACT

To delete the SNMP system contact use the **unset snmp contact** command.

unset snmp contact

6.9.10 VIEWING THE SNMP SETTINGS

To view the SNMP settings use the **get snmp** command with the **settings** option. This will display the current SNMP settings.

- cli-> get snmp settings
- Listening port: 161
- System name: NetSecure 6100
- Location: Lab
- Contact: Jon Smith
- cli->

6.9.11 VIEW THE SNMP COMMUNITY SETTINGS

To view the SNMP community settings use the **get snmp** command with the **community** option. This will display the current SNMP community settings.

- cli-> get snmp community
- Community string: public Host name: 192.168.1.1

6.9.12 VIEW THE SNMP STATISTICS

To view the SNMP statistics use the **get snmp** command with the **statistics** option. This will display the current SNMP statistics.

- cli-> get snmp statistics

- In pkts : 0
- Out pkts : 0
- In bad versions : 0
- In bad community names : 0
- In bad community uses : 0
- In asn parse errors : 0
- In bad types : 0
- In too bigs : 0
- In no such names : 0
- In bad values : 0
- In read onlys : 0
- In gen errs : 0
- In total req vars : 0
- In total set vars : 0
- In get requests : 0
- In get nexts : 0
- In set requests : 0
- In get responses : 0
- In traps : 0
- Out too bigs : 0
- Out no such names : 0
- Out bad values : 0
- Out read onlys : 0
- Out gen errs : 0
- get requests : 0
- Out get nexts : 0

- Out set requests : 0
- Out get responses : 0
- Out traps : 0
- Silent drops : 0
- Proxy drops : 0

GUI Example: View the SNMP statistics

- Logging > SNMP
- Select the Get SNMP Statistics Button

6.9.13 VIEWING THE INTERFACE STATISTICS

To view the interface statistics for a specific physical interface use the **get counter** command and specify the specific interface.

get counter statistics interface {interface name}

Example: To view the interface statistics for the ETH0 interface.

- get counter statistics interface eth0
- cli-> get counter statistics interface eth0
- Hardware counters for interface eth0:
- dos syn drops 0 | dos fin drops 0
- dos icmp drops 0 | dos frag drops 0
- dos udp drops 0 | dos other drops 0
- in pkts 71367 | in bytes 6090575
- in reassembled pkts 0 | in fragment timeout 0
- in short frames 0 | in crc errors 0
- in dropped vlans 0 | in arp pkts 157
- in icmp pkts 0 | in tcp pkts 1450

- in udp pkts 0 | in vlan pkts 0
- in gre pkts 0 | in esp pass-thru pkts 0
- in ah pass-thru pkts 0 | in bad protocol pkts 0
- in policy deny 1000 | in no route 0
- in no sa with policy 0 | in policy permit 6
- in no dip 0 | in bad policy 0
- in ipsec sa fail 0 | in ipsec crypto err 0
- in ipsec esp only 0 | in ipsec esp na 0
- in ipsec esp auth 0 | in ipsec ah 0
- in ipsec replay fail 0 | in ipsec auth fail 0
- out pkts 1821 | out bytes 725315
- out arp pkts 163 |
- out icmp pkts 0 | out tcp pkts 654
- out udp pkts 1004 | out vlan pkts 0
- out gre pkts 0 | out esp pass-thru 0
- out ah pass-thru 0 | out bad protocol pkts 0
- out ipsec replay fail 0 |
- out ipsec crypto busy 0 | out ipsec esp only 0
- out ipsec esp na 0 | out ipsec esp auth 0
- out ipsec ah 0 |

GUI Example: View the interface statistics for the ETH0 interface

- Reports > Counters > Hardware
- Select the Interface Eth0
- Select the Go button

Chapter 7. Virtual Private Networks

This chapter describes the different modes and configuration options available for a virtual private network (VPN). This chapter includes the following topics:

- Virtual Private Networks
- Configuring Manual Key VPN Implementations
- Configuring Internet Key Exchange
- Advanced VPN Configuration Options

7.1 VIRTUAL PRIVATE NETWORKS

Businesses can use a Virtual Private Network (VPN) to communicate and transfer information securely over the Internet. Secure private networks that use VPN technology provide a low-cost infrastructure, enabling increased communication for global business. This infrastructure includes connections for regional offices, branch offices and business partners (refer to Figure 7-1).

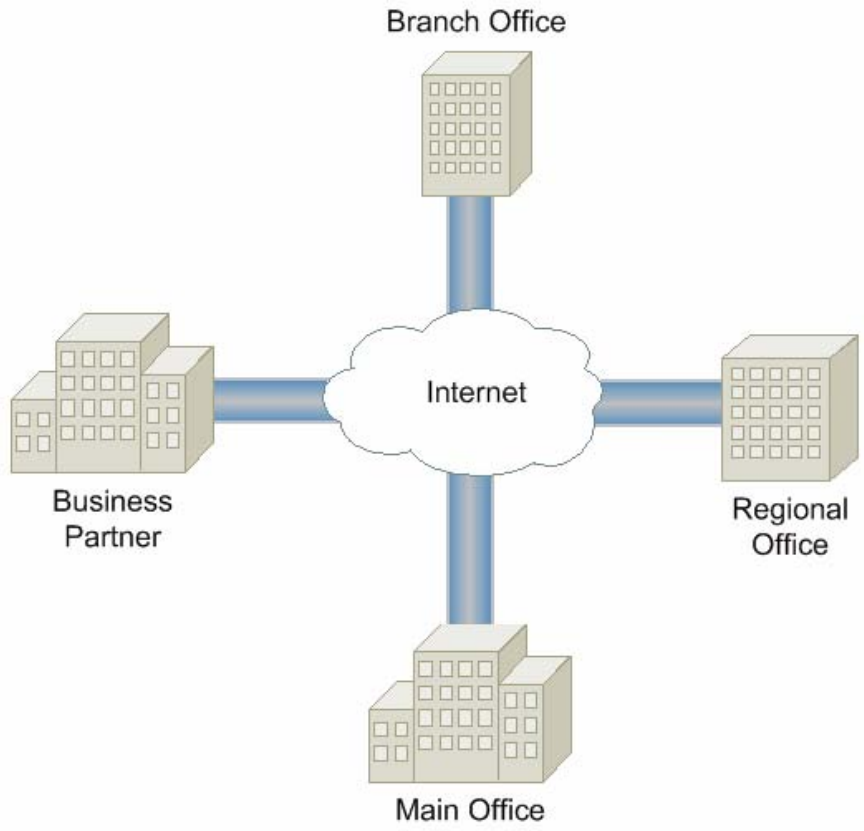


Figure 7-1 VPN Connectivity

7.1.1 ABOUT IP SECURITY (IPSEC)

IPsec is a suite of protocols developed by the Internet Engineering Task Force (IETF) to enable secure exchange at the IP level. The most common implementation of IPsec is seen in VPN deployments. IPsec can be broken down into two different modes and protocols. The modes include Transport and Tunnel and the protocols include AH and ESP.

7.1.2 TRANSPORT MODE

Transport mode is a method by which the data portion of a packet is encrypted, while the IP header information is sent in the clear. The original packet can be authenticated with AH, while the original data can be encrypted with ESP, and the IP header remains in clear text. Figure 7-2 shows VPNs using transport mode.

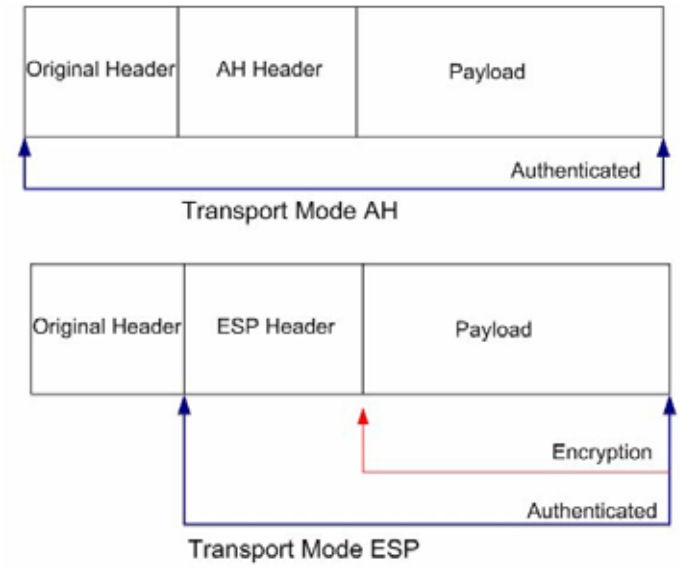


Figure 7-2 VPNs Using Transport Mode

7.1.3 TUNNEL MODE

In tunnel mode (refer toFigure 7-3), all data is encrypted including the IP header. All of the original data is encapsulated into a new IP payload and includes a new IP header. The original packet can be encrypted, authenticated, or both; this is determined by using AH, ESP or a combination of both.

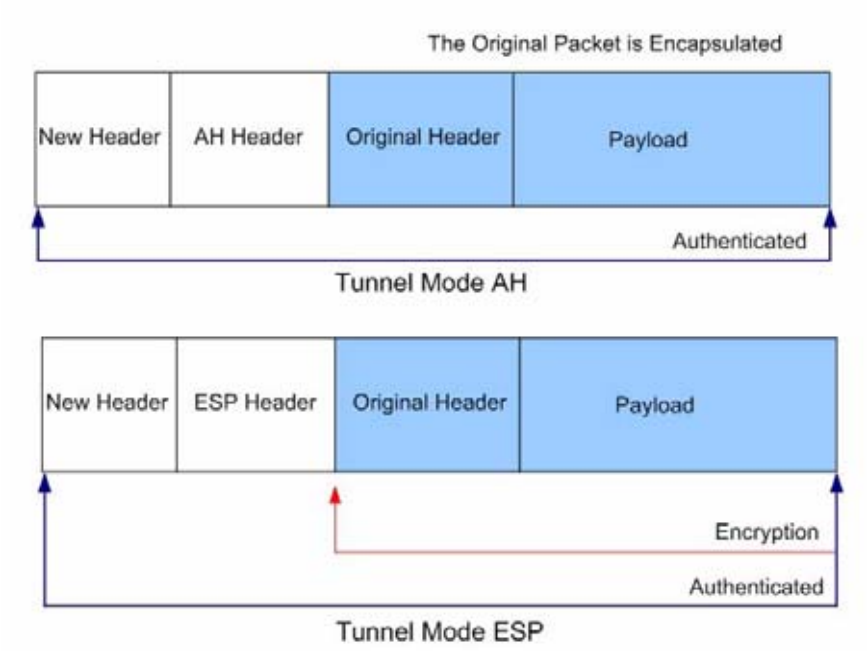


Figure 7-3 Using Tunnel Mode

The AH protocol provides data integrity, authentication, and anti-replay protection. The AH protocol uses a secret key and a hash function— either Message Digest (MD5) or Secure Hash Algorithm-1 (SHA-1)—to authenticate the packet with a checksum calculation or hash-based message authentication code (HMAC). Table 7-1 explains MD5 and SHA1.

Table 7-1 MD5 and SHA-1 Description

Hash Function	Description
MD5	A one-way hash function. This hash function takes variable-length messages and formats them to a fixed length using a 16-byte key to produce a 128-bit hash.
SHA-1	A one-way hash function. This hash function takes variable-length messages and formats them to a fixed length using a 20-byte key to produce a 160-bit hash.

The ESP protocol ensures privacy (encryption), source authentication, and content integrity (authentication). ESP includes the ability to encrypt, encrypt and authenticate, and authenticate only where SHA-1or MD5 provides authentication. Use the following encryption algorithms to encrypt:

- **Data Encryption Standard (DES)**—Uses either a 40- or 56-bit encryption algorithm.
- **Triple DES (3DES)**—Uses a more powerful version of DES encryption. Encrypts the date in three rounds with a 168-bit key.
- **Advanced Encryption Standard (AES)**—An emerging encryption standard that can use a 128-, 192-, or 256-bit encryption key. This new standard supports ease of interoperability with other security appliances as it becomes widely adapted.

7.1.4 THE DIFFIE-HELLMAN GROUP

Users can create a shared secret value using the Diffie-Hellman (DH) group. This value is secure so that the original message can be sent over an insecure medium without sending the secret message along with it. There are a total of three DH groups available for configuration within the VPN policy:

- DH Group 1—768 bit
- DH Group 2—1024 bit
- DH Group 5—1536 bit

It is more secure to use DH group 5, but as you increase the bit modulus it will take longer for the key generation process. Because such a variant exists in the size of the bit modulus, both participants must agree to use the same DH group.

7.1.5 SECURITY ASSOCIATION

Security Association (SA) is a unidirectional agreement between VPN appliances that defines the parameters used to secure the data communication. To allow bi-directional communication, you must define two SAs, one for each direction:

- Key management (manual key, IKE)
- SA lifetime
- Protocol mode
- Security algorithms and keys

7.1.6 SITE-TO-SITE VPN REQUIREMENTS

Site-to-site VPN is a common method used to connect remote offices with a main office over the public Internet. In a site-to-site VPN (refer to Figure 7-4), all hosts in the branch office can communicate and transfer data securely with hosts in the main office. In order to create a secure connection, a security appliance is placed on the edge of each network to provide firewall and VPN functionality.

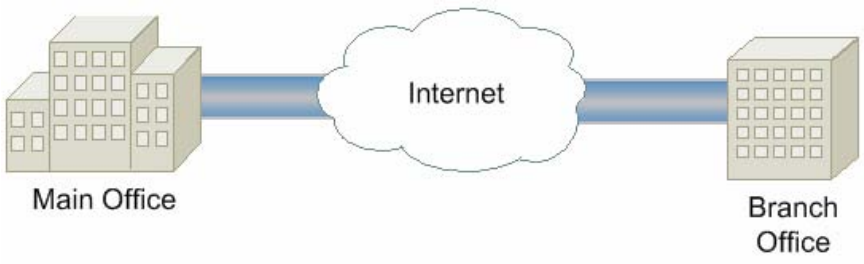


Figure 7-4 Site-to-site VPN

Creating a VPN tunnel between multiple <NetSecure 6100> appliances requires the following configuration:

- The static IP address is assigned to the eth1 interface on each of the appliances.
- The trusted networks connect to the eth0 interface of the appliance.
- The pre-shared secret or pass phrase for the tunnel uses the same configuration for each SA.
- The type of encryption used to encrypt the data is DES, 3DES, or AES.
- The type of authentication used to authenticate the data is MD5 or SHA-1.

7.1.7 VPN SPECIAL CONSIDERATIONS

Before implementing a VPN configuration between two or more networks, consider the following:

- Trusted networks between multiple appliances must have a unique subnet addresses.
- You must properly configure devices connected to the eth0 interface to gain access across the VPN tunnel.
- IP addresses on the eth1 interface of each appliance are required.

7.2 CONFIGURING MANUAL KEY VPN IMPLEMENTATIONS

In a manual key implementation, the VPN tunnel is configured with a static set of encryption keys and authentication keys.

7.2.1 CREATING MANUAL KEY VPN TUNNELS

Use the **set vpn** command with the **manual** option to configure a manual key VPN:

set vpn {name_str} manual {local-spi} {remote-spi} gateway {ip-addr} outgoing-interface {interface} {protocol} {encryption} key {encryption_key} auth {authentication} key {authentication_key}

Table lists the required parameters to configure one side of a manual key VPN tunnel. Refer to the *CLI Reference Guide and Command Descriptions* for additional manual key parameters.

Table 7-2 Required Manual Key VPN Parameters

Parameter	Description
vpn {name_str}	VPN Tunnel Name—Name that uniquely identifies the VPN tunnel.
manual	Manual key VPN—Specifies the tunnel as manual.
{local-spi}, {remote-spi}	Security Parameter Index (SPI)— Hexadecimal value (four to ten characters in length).
gateway {ip-addr}	IPsec Gateway—IP address of fully qualified domain name.
outgoing-interface {interface}	Outgoing Interface—The interface for which the VPN tunnel is bound.
{protocol}	Protocol—AH or ESP.
{encryption}	Encryption—DES, 3DES, or AES (128, 192, and 256).
key {encryption_key}	Encryption Key—Hexadecimal value (l16 characters in length).

Parameter	Description
auth {authentication}	Authentication—SHA-1 or MD5.
key {authentication_key}	Authentication Key—Hexadecimal value (32 characters in length).
Policy Requirements	
Local Network	The local network attached to the <NetSecure 6100>.
Destination Network	Network to which the VPN tunnel will terminate.

7.2.2 CREATING SECURITY POLICY WITH THE VPN TUNNELS

A VPN tunnel that is created is used in a security policy that specifies the local and destination networks. Traffic that matches the source and destination networks specified in policies with the **vpn** option is encrypted or decrypted. The **set policy** command with the **vpn** option specifies the VPN tunnel in the security policy to use for encryption and decryption:

set policy top name {name_str} from {zone} to {zone} {remote network} {local network} {service} tunnel vpn {name_str}

Table 7-3 explains these parameters in this command. Refer to the CLI Reference Guide and Command Descriptions for additional policy parameters.

Table 7-3 Policy Requirements for Manual Key VPN

Parameter	Description
top	Move the tunnel policies to the top of the policies list.
name {name_str}	Name that uniquely identifies the tunnel policy.
from {zone}	Source zone from which the VPN traffic originates.
To {zone}	Destination zone for the VPN traffic.
{remote network}	Specifies the destination network for the VPN tunnel.
{local network}	Specifies the local network for the VPN tunnel.
{service}	Specifies the services enabled to pass through the VPN tunnel.
tunnel	Action that specifies the policy to encrypt and decrypt traffic.

Parameter	Description
vpn {name_str}	Binds the tunnel policies to the specified manual key VPN tunnel.

[NOTE] Manual key VPN requires two policies for each VPN tunnel: one policy that allows encryption and decryption on ingress traffic and another policy that allows encryption and decryption on egress traffic.

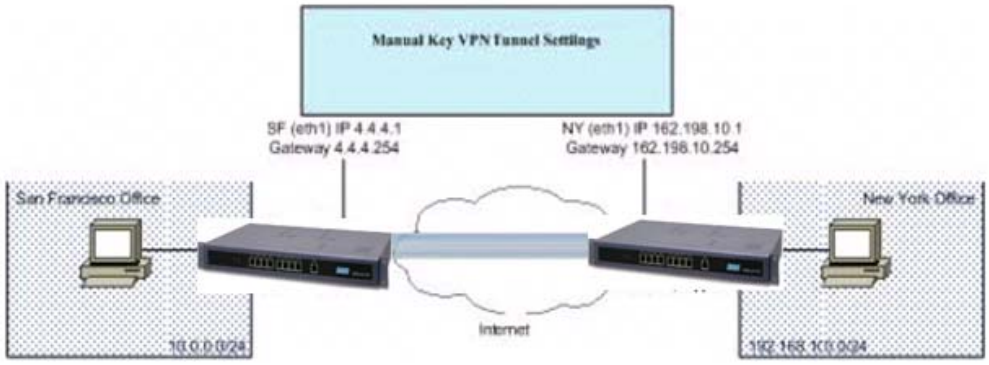


Figure 7-5 Example of Manual Key VPN

Table 7-4 Example of Encryption and Authentication Settings

Manual Key Setting	Value
Encryption	AES128
Authentication	SHA-1
Protocol	ESP
Local SPI	1230
Remote SPI	1230
Encryption Key	11112222333344445555666677778888
Authentication Key	1111222233334444555566667777888899999aaaa

Follow these steps to configure the required VPN tunnels in Table 7-2.

- Define your security zone and interface IP.
- Create address objects for the local and remote end points.
- Define the remote gateway and SPI to be used, refer to Table 7-2.
- Define the authentication and encryption keys to be used, refer to Table 7-2.
- Set a route for the VPN.

- Create policies to allow traffic to ingress and egress though the newly created VPN tunnel.

Example: Manual key VPN implementationm, New York office

Refer to Figure 7-4 and Figure 7-5 for the following example of a manual key VPN implementation.

Interfaces

- set interface eth0 zone trust
- set interface eth0 ip 192.168.100.1/24
- set interface nat
- set interface eth1 zone untrust
- set interface eth1 ip 162.198.10.1/24

Addresses

- set address trust nyo 192.168.100.0/24
- set address untrust San Francisco 10.0.0.0/24

VPN

- set vpn to_sanfrancisco manual 1230 1230 gateway 4.4.4.1
- outgoing-interface eth1 esp aes128 key 1111222233334444
- auth sha-1 key 11112222333344445555666677778888

Routing

- set route trust route 0.0.0.0/0 interface eth1 gateway 162.198.10.254

Policies:

- set policy top name vpnto_sanfrancisco from trust to untrust nyo San Francisco any tunnel vpn sfo_nyo
- set policy top name vpnfrom_sanfrancisco from untrust to trust San Francisco nyo any tunnel vpn sfo_nyo

- save

GUI Example: Manual key VPN implementationm, New York office

Interfaces

- Network > Interface > Edit (for ethernet0)
- Enter the following, then click **Apply**:
  Zone Name: Trust
  IP Address/Netmask: 192.168.100.1/24
  Interface Mode: NAT
- Network > Interface > Edit (for eth1): Enter the following, then click **Apply**:
  Zone Name: Untrust
  IP Address/Netmask: 162.198.10.1/24

Addresses

- Objects > Address Objects > Add Object
- Enter the following, then click **Apply**:
  Name: NYO
  IP Address/Netmask: 192.168.100.0/24
  Zone: Trust
- Objects > Address Objects > Add Object 4 Enter the following, then click **Apply**:
  Name: San Francisco
  IP Address/Netmask: 10.0.0.0/24
  Zone: Untrust

VPN

- VPN > Manual Key Edit 2 Enter the following, then click **Apply**:
  Tunnel Name: to_sanfrancisco
  Gateway IP: 4.4.4.1
  Outgoing interface: eth1
  Local SPI: 1230
  Remote SPI: 1230
  Encryption Algorithm: aes-128

Hex Key: 1111222233334444
Authentication Algorithm: sha-1
Hex Key: 11112222333344445555666677778888

Routing

- Network > Route Add
- Enter the following, then click **Apply**:
  Network Address: 0.0.0.0
  Netmask: 0
  Interface: eth1
  Gateway: 162.198.10.254

Policies

- Policy > Configuration Edit
- Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Trust
  Destination Zone: Untrust
  Source Address: NYO
  Destination Address: San Francisco
  Service: Any
  Tunnel VPN From: SF
- Policy > Configuration Edit: Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Untrust
  Destination Zone: Trust
  Source Address: San Francisco
  Destination Address: NYO
  Service: Any
  Tunnel VPN From: SF

Example: Manual key VPN implementation, San Francisco office

Interfaces

- set interface eth0 zone trust
- set interface eth0 ip 10.0.0.0/24
- set interface nat
- set interface eth1 zone untrust
- set interface eth1 ip 4.4.4.1

Addresses

- set address trust sfo 10.0.0.0/24
- set address untrust New York 192.168.100.0/24

VPN

- set vpn to_newyork manual 1230 1230 gateway 4.4.4.1
- outgoing-interface eth1 esp-aes128 key 1111222233334444
- auth sha-1 key 11112222333344445555666677778888

Routing

- set route trust route 0.0.0.0/0 interface eth1 gateway 4.4.4.254

Policies:

- set policy top name vpnto_newyork from trust to untrust sfo New York any tunnel vpn sfo_nyo
- set policy top name vpnfrom_newyork from untrust totrust New York sfo any tunnel vpn sfo_nyo
- save

GUI Example: Manual key VPN implementation, San Francisco office

Interfaces

- Network > Interface > Edit (for ethernet0)

- Enter the following, then click **Apply**:
  Zone Name: Trust
  IP Address/Netmask: 10.0.0.0/24
  Interface Mode: NAT

- Network > Interface > Edit (for eth1): Enter the following, then click **Apply**:
  Zone Name: Untrust
  IP Address/Netmask: 4.4.4.1/24

Addresses

- Objects > Address Objects > Add Object

- Enter the following, then click **Apply**:
  Name: SFO
  IP Address/Netmask: 10.0.0.0/24
  Zone: Trust

- Objects > Address Objects > Add Object

- Enter the following, then click **Apply**:
  Name: New York
  IP Address/Netmask: 192.168.100.0/24
  Zone: Untrust

VPN

- VPN > Manual Key Edit

- Enter the following, then click **Apply**:
  Tunnel Name: to_newyork
  Gateway IP: 4.4.4.1
  Outgoing interface: eth1
  Local SPI: 1230
  Remote SPI: 1230
  Encryption Algorithm: aes-128
  Hex Key: 1111222233334444
  Authentication Algorithm: sha-1
  Hex Key: 11112222333344445555666677778888

Routing

- Network > Route Add
- Enter the following, then click **Apply**:
  Network Address: 0.0.0.0
  Netmask: 0
  Interface: eth1
  Gateway: 4.4.4.254

Policies

- Policy > Configuration Edit
- Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Trust
  Destination Zone: Untrust
  Source Address: SFO
  Destination Address: New York
  Service: Any
  Tunnel VPN From: SF
- Policy > Configuration Edit
- Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Untrust
  Destination Zone: Trust
  Source Address: New York
  Destination Address: SFO
  Service: Any
  Tunnel VPN From: SF

7.2.3 DELETING MANUAL KEY VPN TUNNELS

Use the **unset vpn** command to delete a manual key VPN tunnel:

unset vpn {vpn_name}

7.2.4 MODIFYING MANUAL KEY VPN TUNNELS

To modify a manual key VPN tunnel, first delete the tunnel using the **unset vpn** command and then add the tunnel again with the appropriate changes using the **set vpn** command.

Example: Modifying a manual key VPN tunnel

Use the **unset vpn** command to change the name of the VPN tunnel previously created on an appliance from to_newyork to sales_office:

- unset vpn to_newyork
- set vpn Sales_Office manual local spi 1230 remote spi 1230 gateway 4.4.4.1 outgoing-interface eth1 esp-aes128 key 1111222233334444 auth sha-1 key 11112222333344445555666677778888
- save

7.3 CONFIGURING INTERNET KEY EXCHANGE

Internet Key Exchange (IKE) VPN uses a pre-shared secret to allow the creation of a VPN tunnel between two or more VPN appliances. During the IKE negotiation phase, the pre-shared secret creates keys that encrypt and decrypt packets. Unlike manual key implementations, IKE VPNs have an SA lifetime. This lifetime determines when the current keys being used for encryption and decryption expire. After the SA expires, the IKE session uses the pre-shared secret to randomly generate new keys for the encryption and decryption process. At a minimum, you need to define an IKE Phase 1 proposal, IKE Phase 2 proposal, IKE gateway and security policy in order to configure an IKE VPN tunnel using a pre-shared secret.

7.3.1 CREATING IKE PHASE 1 AND PHASE 2 PROPOSALS

Use the **set ike p1-proposal** or **set ike p2-proposal** commands to create an IKE Phase 1 proposal or IKE Phase 2 proposal, respectively:

- set ike p1-proposal {name_str} preshare {dh_group} {protocol} {encryption}
- set ike p2-proposal {name_str} {dh_group} {protocol} {encryption} {authentication} {lifetime}
- set ike gateway {name_str} ip {address_str} {main|aggressive} outgoing-interface {name} preshare {name_str} proposal {p1_name}
- set vpn {name_str} gateway {gw_name} proposal {p2_name}

Table 7-5 shows the required Phase 1 and Phase 2 Proposal Settings.

Table 7-5 Required Phase 1 and Phase 2 IKE Proposal Settings

Tunnel Name	Name that uniquely identifies the VPN tunnel
IPSec Gateway	IP address or Fully Qualified Domain Name
Pre-Shared Secret	Pass phrase used to authenticate VPN appliance.
IKE Identity	IPv4 address, e-mail address or FQDN

Tunnel Name	Name that uniquely identifies the VPN tunnel
Phase 1	Exchange proposal to determine how to authenticate and secure the channel.
Mode Exchange	Main or Aggressive
DH Group	1, 2 or 5
Protocol	AH, ESP
Encryption	DES, 3DES or AES
Authentication	MD5, SHA-1
SA Life Time	Lifetime for a single set of encryption keys.
Phase 2	Exchange that allows an SA to be created, allowing for the secure transmission of data using IPsec.
Encryption	DES, 3DES or AES
Authentication	MD5 or SHA-1
DH Group	1, 2 or 5
Protocol	AH or ESP
SA Life Time	Lifetime for a single set of encryption keys
Prefect Forward Secrecy	Generates a new key for every message sent through an SA.
Local Network	The local network attached to the VF-2112.
Destination Network	Network to which the VPN tunnel will terminate

Figure 7-6 shows an IKE VPN using a pre-shared secret.

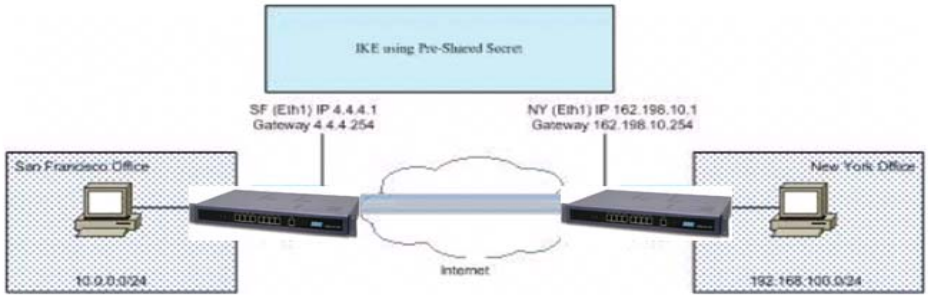


Figure 7-6 IKE VPN Using a Pre-Shared Secret

Table 7-6 shows the IKE Encryption and Authentication Settings.

Table 7-6 IKE Encryption and Authentication Settings

Parameter	Description
Encryption	AES128
Authentication	SHA-1

Parameter	Description
DH Group	5
SA Lifetime	28800
Pre-shared Secret	password

7.3.2 CONFIGURING AN IKE TUNNEL USING A PRE-SHARED SECRET

Setting up a VPN tunnel using IKE requires the following steps:

- Define your security zone interface IP.
- Create address objects for the local and remote end points.
- Define the remote gateway and key exchange mode along with pre-shared secret.
- Create the IKE VPN.
- Set a route for the VPN.
- Create policies to allow traffic to ingress and egress though the newly created VPN tunnel.

Example: New York office using IKE

Interfaces

- set interface eth0 zone trust
- set interface eth0 ip 192.168.100.1/24
- set interface nat
- set interface eth1 zone untrust
- set interface eth1 ip 162.198.10.1/24

Addresses

- set address trust ny_local 192.168.100.0/24
- set address untrust sf_destination 10.0.0.0/24

VPN

- set ike p1 proposal encryptaesp1 preshare group5 esp aes 128 sha-1
- set ike p2 proposal encryptaesp2 preshare group5 esp aes 128 sha-1 seconds 28800
- set ike gateway to_sanfrancisco address 4.4.4.1 main outgoing-interface eth1 preshare password proposal encryptaesp1
- set vpn sfo_nyo gateway to_sanfrancisco proposal encryptaesp2

Routing

set route trust route 0.0.0.0/0 interface eth1 gateway 162.198.10.254

Policies

- set policy top name vpnto_sanfrancisco from trust to untrust ny_local sf_destination any tunnel vpn sfo_nyo
- set policy top name vpnfrom_sanfrancisco from untrust to trust sf_destination ny_local any tunnel vpn sfo_nyo
- save

GUI Example: New York office using IKE

Interfaces

- Network > Interface > Edit (for ethernet0)
- Enter the following, then click **Apply**:
  Zone Name: Trust
  IP Address/Netmask: 192.168.100.1/24
  Interface Mode: NAT
- Network > Interface > Edit (for eth1)
- Enter the following, then click **Apply**:
  Zone Name: Untrust
  IP Address/Netmask: 162.198.10.1/24

Addresses

- Objects > Address Objects > Add Object
- Enter the following, then click **Apply**:
  Name: ny_local
  IP Address/Netmask: 192.168.100.0/24
  Zone: Trust
- Objects > Address Objects > Add Object: Enter the following, then click **Apply**:
  Name: sf_destination
  IP Address/Netmask: 10.0.0.0/24
  Zone: Untrust

VPN

- VPN > Phase 1 Proposal Edit
- Enter the following, then click **Apply**:
  Name: encryptaesp1
  Authentication Method: PSK
  DH Group: Group-5
  Encryption Algorithm: aes-128
  Hash Algorithm: SHA-1
- VPN > Phase 2 Proposal Edit
- Enter the following, then click **Apply**:
  Name: encryptaesp2
  PSF: PSF-Group5
  Encryption Algorithm: aes-128
  Hash Algorithm: SHA-1
  Seconds: 28800
- VPN > IKE Gateway Edit
- Enter the following, then click **Apply**:
  Gateway name: to_sanfrancisco
  Remote IPsec Gateway IP: 4.4.4.1
  Outgoing interface: eth1
  Phase 1 Proposal: encryptaesp1

Routing

- Network > Route Add
- Enter the following, then click **Apply**:
  Network Address: 0.0.0.0
  Netmask: 0
  Interface: eth1
  Gateway: 162.198.10.254

Policies

- Policy > Configuration Edit
- Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Trust
  Destination Zone: Untrust
  Source Address: ny_local
  Destination Address: sf_destination
  Service: Any
  Tunnel VPN From: SF
- Policy > Configuration Edit
- Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Untrust
  Destination Zone: Trust
  Source Address: sf_destination
  Destination Address: ny_local
  Service: Any
  Tunnel VPN From: SF

Example: San Francisco office using IKE

Interfaces

- set interface eth0 zone trust
- set interface eth0 ip 10.0.0.0/24
- set interface nat
- set interface eth1 zone untrust
- set interface eth1 ip 4.4.4.1

Addresses

- set address trust sf_local 10.0.0.0/24
- set address untrust ny_destination 192.168.100.0/24

VPN

- set ike p1 proposal encryptaesp1 preshare group5 esp aes128 sha-1
- set ike p2 proposal encryptaesp2 preshare group5 esp aes128 sha-1 seconds 28800
- set ike gateway to_newyork address 162.198.10.1 main outgoing-interface eth1 preshare password proposal encryptaesp1
- set vpn sfo_nyo gateway to_newyork proposal encryptaesp2

Routing

- set route trust route 0.0.0.0/0 interface eth1 gateway 4.4.4.254

Policies

- set policy top name vpnto_newyork from trust to untrust sf_local ny_destination and tunnel vpn sfo_nyo
- set policy top name vpnfrom_newyork from untrust to trust ny_destination sf_local any tunnel vpn sfo_nyo
- save

GUI Example: San Francisco office using IKE

Interfaces

- Network > Interface > Edit (for ethernet0)
- Enter the following, then click **Apply**:
  Zone Name: Trust
  IP Address/Netmask: 10.0.0.0/24
  Interface Mode: NAT
- Network > Interface > Edit (for eth1)
- Enter the following, then click **Apply**:
  Zone Name: Untrust
  IP Address/Netmask: 4.4.4.1/24

Addresses

- Objects > Address Objects > Add Object
- Enter the following, then click **Apply**:
  Name: sf_local
  IP Address/Netmask: 10.0.0.0/24
  Zone: Trust
- Objects > Address Objects > Add Object
- Enter the following, then click **Apply**:
  Name: ny_destination
  IP Address/Netmask: 192.168.100.0/24
  Zone: Untrust

VPN

- VPN > Phase 1 Proposal Edit
- Enter the following, then click **Apply**:
  Name: encryptaesp1
  Authentication Method: PSK
  DH Group: Group-5
  Encryption Algorithm: aes-128
  Hash Algorithm: SHA-1
- VPN > Phase 2 Proposal Edit

- Enter the following, then click **Apply**:
  Name: encryptaesp2
  PSF: PSF-Group5
  Encryption Algorithm: aes-128
  Hash Algorithm: SHA-1
  Seconds: 28800

- VPN > IKE Gateway Edit: Enter the following, then click **Apply**:
  Gateway name: to_sanfrancisco
  Remote IPsec Gateway IP: 4.4.4.1
  Outgoing interface: eth1
  Phase 1 Proposal: encryptaesp1

Routing

- Network > Route Add

- Enter the following, then click **Apply**:
  Network Address: 0.0.0.0
  Netmask: 0
  Interface: eth1
  Gateway: 4.4.4.254

Policies

- Policy > Configuration Edit

- Enter the following, then click **Apply**:
  Enable Policy
  Location: Top
  Action: Tunnel
  Source Zone: Trust
  Destination Zone: Untrust
  Source Address: sf_local
  Destination Address: ny_destination
  Service: Any
  Tunnel VPN From: SF

- Policy > Configuration Edit

- Enter the following, then click **Apply**:
  Enable Policy

Location: Top
Action: Tunnel
Source Zone: Untrust
Destination Zone: Trust
Source Address: ny_destination
Destination Address: sf_local
Service: Any
Tunnel VPN From: SF

7.3.2.1 DELETING AN IKE VPN TUNNEL

To delete an IKE VPN tunnel you will use the unset ike command to delete phase 1 and unset vpn command to delete phase 2.

- unset ike gateway {name_str}
- unset vpn {name_str}

7.3.2.2 MODIFYING AN IKE VPN TUNNEL

To modify an IKE VPN tunnel you must first delete the tunnel information and re-add the tunnel with the appropriate changes.

Example: Modifying an IKE VPN tunnel

To change the VPN tunnel name on a previously created VPN tunnel from “to_newyork” to “New_York:”

- unset ike gateway to_newyork
- unset vpn sfo_nyo
- set ike gateway New_York address 162.198.10.1 main outgoing-interface eth1 preshare password proposal encryptaesp1
- set vpn sfo_nyo gateway to_newyork proposal encryptaesp2
- save

GUI Example: Modifying an IKE VPN tunnel

- VPN > IKE Gateways
- Select the following, then click **Apply**:
  Remove: to_newyork
- VPN > IKE Settings
- Select the following, then click **Apply**:
  Remove: sfo_nyo
- VPN > IKE Gateway Edit
- Enter the following, then click **Apply**:
  Gateway name: New_York
  Remote IPsec Gateway IP: 162.198.10.1
  Outgoing interface: eth1
  Phase 1 Proposal: encryptaesp1

7.3.3 TRANSPARENT MODE VPN DEPLOYMENT

[NOTE] For information on Transparent Mode, see 3.4.4 CONFIGURING TRANSPARENT MODE.

Figure 7-7 shows a VPN setup between two appliances running in transparent mode.

Figure 7-7 VPN in Transparent Mode

In Figure 7-7 the appliances will be used in transparent mode, but will also terminate VPN between two sites.

Configuration Elements	VF4000 A	VF4000 B
Trust Zone	eth0 0.0.0.0	eth0 0.0.0.0
Untrust Zone	eth1 0.0.0.0	eth1 0.0.0.0
Addresses	Local_lan 10.0.0.0/2, Trust Peer_lan 172.16.10.0/24, Untrust	Local_lan 172.16.10.0/24, Trust Peer_lan 10.0.0.0/24, Untrust
IKE Gateway	GWA 10.0.0.100, preshared password	GWB 172.16.10.100, preshared password
Policies	local_lan -> peer_lan, any service, vpn1 peer_lan -> local_lan, any service, vpn1	local_lan -> peer_lan, any service, vpn1 peer_lan -> local_lan, any service, vpn1
Management Interface The br0 interface must be on the Untrust Zone. This determines the direction in which the encrypted traffic will flow.	Br0: 10.0.0.110 Zone: Untrust	Br0: 172.16.10.100 Zone: Untrust
Configuration Elements	VF4000 A	VF4000 B
External Router IP	10.0.0.5	172.16.10.5
Default Route	0.0.0.0/0 eth br0, gateway 10.0.0.5	0.0.0.0/0eth br0, gateway 172.16.10.5

7.3.4 CONFIGURATION OF VF A

- set interface br0 ip 10.0.0.100/24
- set interface br0 zone untrust
- set interface eth0 ip 0.0.0.0/0
- set interface eth0 transparent
- set interface eth0 zone trust
- set interface eth1 ip 0.0.0.0/0

- set interface eth1 transparent
- set interface eth1 zone untrust

- set route 0.0.0.0/0 interface br0 gateway 10.0.0.5 metric 1

- set address trust local_lan 10.0.0.0/24
- set address untrust peer_lan 172.16.10.0/24

- set ike gateway gw1 address 172.16.10.100 main outgoing-interface br0 preshare
- password sec-level compatible
- set vpn vpn1 gateway gw1 sec-level compatible

- set policy top from trust to untrust local_lan peer_lan any tunnel vpn
- vpn1
- set policy top from untrust to trust peer_lan local_lan any tunnel vpn
- vpn1

7.3.5 CONFIGURATION OF VF B

- set interface br0 ip 172.16.10.100/24
- set interface br0 zone untrust
- set interface eth0 ip 0.0.0.0/0
- set interface eth0 transparent
- set interface eth0 zone trust
- set interface eth1 ip 0.0.0.0/0
- set interface eth1 transparent

- set interface eth1 zone untrust

- set route 0.0.0.0/0 interface br0 gateway 172.16.10.5metric 1

- set address trust local_lan 172.16.10.0/24
- set address untrust peer_lan 10.0.0.0/24

- set ike gateway gw1 address 10.0.0.100 main outgoing-interface br0 preshare
- password sec-level compatible
- set vpn vpn1 gateway gw1 sec-level compatible

- set policy top from trust to untrust local_lan peer_lan any tunnel vpn
- vpn1
- set policy top from untrust to trust peer_lan local_lan any tunnel vpn
- vpn1

7.4 ADVANCED VPN CONFIGURATION OPTIONS

Some advanced options are available, but not always required to be configured for each tunnel. They include dead peer detection (DPD), DF Bit settings, NAT-Traversal (NAT-T) perfect forward secrecy (PFS) and anti-replay protection.

7.4.1 DEAD PEER DETECTION (DPD)

Dead Peer Detection (DPD) allows two or more VPN appliances to send communication to determine the validity of a VPN tunnel. Without DPD a situation could arise where communication between one or more VPN appliances is interrupted unexpectedly, causing the VPN tunnel to not respond or allow traffic to

pass. This service interruption could last until the SA lifetime expires, if DPD were not used. To configure DPD use the **set ike** command along with the **DPD** option to set how many missed r-u-there message are allowed before the VPN tunnel is torn down the rebuilt.

- set ike gateway {name_str} dpd always-send
- set ike gateway {name_str} dpd interval {number}
- set ike gateway {name_str} dpd retry {number}

7.4.2 NAT-TRAVERSAL (NAT-T)

NAT-T allows encrypted VPN traffic to be encapsulated as a UDP datagram using port 500. During phase 1 of the VPN negotiation the VPN appliance's will determine automatically if any device along their path has applied NAT to the VPN packets. If NAT is applied along the specific path the VPN appliances will then encapsulate the VPN traffic as UDP datagrams using port 500.

To enable NAT-Traversal, use the **set ike** command.

set ike gateway {name_str} nat-traversal

7.4.3 PERFECT FORWARD SECRECY (PFS)

PFS is a condition in which an encryption system changes encryption keys often and ensures that no two sets of keys have any relation. Unless specified all new **p2-proposal**s defined have PFS enabled. To disable PFS you will use the **set ike** command with the **no-pfs** option, to disable PFS for the defined **p2-proposal**.

- set ike p2-proposal {name_str} no-pfs preshare
- {dh_group} {protocol} {encryption} {authentication}
- {lifetime}

[NOTE] PFS must be enabled on both ends of a VPN configuration.

7.4.4 REPLAY PROTECTION

Replay protection allows the <NetSecure 6100> to check the sequence numbers of the VPN packets, to determine if the packet has been received or not. If the packet does not fit into a specific number sequence the packet will dropped. Replay protection will detect and protect against man-in-the-middle attacks. Replay detection is enabled by default on all IKE VPN tunnels.

To disable replay protection, use the **set vpn** command with the **no-replay** option.

set vpn {name_str} gateway {gw_address} no-replay

7.4.5 VIEW A VPN TUNNEL

To view the current VPN tunnels use the **get vpn** command. You can view all tunnels, specified by name, or type using the **auto** or **manual** options. Auto will show all tunnels using IKE, while manual will show all Manual Key tunnels.

get vpn {name_str| auto| manual}

Example: To view the VPN tunnel "TO_NEWYORK"

get vpn to_newyork

GUI Example: To view the VPN tunnel "TO_NEWYORK"

- VPN > IKE Settings
- Select the following, then click **Apply**:
  Edit (to_newyork)

7.4.6 VIEW IKE INFORMATION

To view IKE information, l use the **get ike** command with the option to view the gateways, p1-proposals, p2-proposals, cookies and id-modes.

7.4.7 VIEW IKE GATEWAY

Using the **get ike gateway** command you can view the current IKE information including current id, gateway name, gateway id, mode and proposal information. Optionally you can get this information for a specific tunnel by specifying the tunnel name.

get ike gateway {name_str}

7.4.8 VIEW IKE PHASE 1 PROPOSALS

To view the IKE phase 1 proposal information, use the **get ike p1proposal** command. Optionally you can specify by name the proposal to view.

get ike p1-proposal{name_str}

7.4.9 VIEW IKE PHASE 2 PROPOSALS

To view the IKE phase 2 proposal information, use the **get ike p2proposal** command. Optionally you can specify by name the proposal to view.

get ike p2-proposal {name_str}

Chapter 8. Routing

This chapter describes the routing options available for configuration on the security appliance. This chapter includes the following topics:

- Static Routes
- Setting the Default Route
- Displaying Route Information
- Routing Information Protocol (RIP)
- Configuring RIP
- Enabling and Disabling RIP on Interfaces
- Disable Route Summarization
- Enable or Disable Split Horizon
- Enable RIP Authentication
- Accepting Packets with Non-Zero Reserved Fields

8.1 STATIC ROUTES

An implicit or explicit route must be defined in the routing table for traffic to move between interfaces on the appliance. The destination network, interface, and gateway define this route. Networks that are directly attached to an interface on the appliance have an implicit route automatically created in the routing table. Networks without an implicit route require a static route that identifies the next hop gateway and interface to forward traffic going to the destination network.

In Figure 8-1, a static route is configured on the appliance to forward traffic from workstations on the *10.0.0.0/24* network to a server on the

10.0.100.0/24 network. The static route identifies 10.0.0.100 as the gateway address for all traffic going to the 10.0.100.0/24 network.

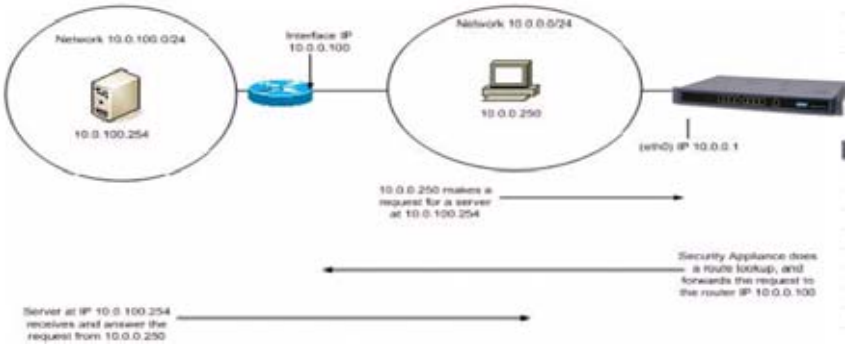

Network 10.0.100.0/24
10.0.100.254
Interface IP
10.0.0.100
Network 10.0.0.0/24
10.0.0.250
(eth0) IP 10.0.0.1
10.0.0.250 makes a request for a server at 10.0.100.254
Security Appliance does a route lookup, and forwards the request to the router IP 10.0.0.100
Server at IP 10.0.100.254 receives and answer the request from 10.0.0.250

Figure 8-1 Using a Static Route

8.1.1 ADDING STATIC ROUTES

Use the **set route** command with the **gateway** and **interface** options to add a static route:

set route {ip_addr/mask} gateway {ip_addr} interface {interface name}

Example: Adding a static route

In the network described in Figure 8-1, a static route is added to allow hosts on the 10.0.0.0/24 network to access a server with the IP address of 10.0.100.254:

- set route 10.0.100.0/24 gateway 10.0.0.100 interface eth0
- save

GUI Example: Adding a static route

- Network > Routing Add
- Enter the following, then click **Apply**:
  Network address: 10.0.100.0
  Netmask: 24
  Interface: etho0
  Gateway: 10.0.0.100

8.1.2 DELETING STATIC ROUTES

Use the **unset route** command to delete a static route:

unset route {ip_addr/mask} gateway {ip_addr} interface{interface name}

8.1.3 MODIFYING STATIC ROUTES

To modify an existing static route, first delete the route and then add a new route entry with the desired route changes.

Example: Modifying a static route

Modify the gateway on a previously created static route from *10.0.0.100* to *10.0.0.20*:

- unset route 10.0.100.0/24 gateway 10.0.0.100 interface eth0
- set route 10.0.100.0/24 gateway 10.0.0.200 interface eth0
- save

GUI Example: Modifying a static route

- Network > Routing
- Select the following, then click **Apply**:
  Remove: 10.0.100.0
- Network > Routing Add
- Enter the following, then click **Apply**:
  Network address: 10.0.200.0
  Netmask: 24
  Interface: etho0
  Gateway: 10.0.0.100

8.2 SETTING THE DEFAULT ROUTE

If a specific route for traffic is unknown to a server or a routing table, the default route forwards all traffic to the default interface you define.

Use the **set route** command to define the default route for all traffic:

set route 0.0.0.0/0 interface {interface name} gateway {ip_addr}

Example: Setting the default route

Configure the default route on the appliance in Figure 8-1 to use the eth1 interface and a gateway of 4.4.4.1, which is the IP address of the next hop gateway:

- set route 0.0.0.0/0 gateway 4.4.4.1 interface eth1
- save

GUI Example: Setting the default route

- Network > Routing Add
- Enter the following, then click **Apply**:
  Network address: 0.0.0.0
  Netmask: 0
  Interface: etho1
  Gateway: 4.4.4.1

8.3 DISPLAYING ROUTE INFORMATION

Use the **get route** command to display all routes on the appliance:

```
get route
```

Figure 8-2 shows an example of the output that appears when you use the **get route** command.

```
get route
Dest-Routes for <> (14 entries)
--------------------------------------------------------------------------------------------------
C - Connected     S - Static      A - Auto-Exported    I – Imported  R – RIP

P – Permanent     iB – IBGP       eB –EBGP     O – OSPF

E1-OSPF external type 1           E2 - OSPF external type 2
--------------------------------------------------------------------------------------------------

IP-Prefix          Interface  Gateway          P    Distance    Metri

64.79.127.64/32    eth1       0.0.0.0          C    0           0
64.79.127.67/32    eth1       0.0.0.0          C    0           0
64.79.127.71/32    eth1       0.0.0.0          C    0           0
64.79.127.64/29    eth1       0.0.0.0          C    0           0
192.168.105.0/24   eth0       192.168.65.240   S    1           1
192.168.115.0/24   eth0       192.168.65.240   S    1           1
192.168.215.0/24   eth0       192.168.65.240   S    1           1
192.168.154.0/24   eth0       192.168.65.240   S    1           1
192.168.145.0/24   eth0       192.168.65.240   S    1           1
192.168.65.0/32    eth0       0.0.0.0          C    0           0
192.168.65.230/32  eth0       0.0.0.0          C    0           0
192.168.65.255/32  eth0       0.0.0.0          C    0           0
192.168.65.0/24    eth0       0.0.0.0          C    0           0
0.0.0.0/0          eth1       64.79.127.65     S    1           1
```

Figure 8-2 Get Route Command Output

Use the **get route** command with the prefix option and **ip_addr** to display route information for a specific IP address:

get route ip {ip_addr}

GUI Example: Get route all

- Network > Routing > Route
- Shows current routing information

Figure 8-3 displays an example of the output that appears when you use the **get route** command with the **ip_addr** option.

```
get route 192.168.65.0/24
Dest-Routes for <> (1 entries)
-------------------------------------------------------------------------------------------------
C – Connected    S – Static     A - Auto-Exported   I – Imported  R – RIP
P – Permanent    iB – IBGP      eB –EBGP    O – OSPF
E1 -OSPF external type 1        E2 - OSPF external type 2
-------------------------------------------------------------------------------------------------
IP-Prefix          Interface  Gateway      P   Distance        Metri
-------------------------------------------------------------------------------------------------
192.168.65.0/24    eth        0 0.0.0.0    C       0               0
```

Figure 8-3 Get Route Command with ip_addr option Output

8.4 ROUTING INFORMATION PROTOCOL (RIP)

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols because a variety of RIP-like routing protocols proliferated, some of which even used the same name! RIP and the myriad RIP-like protocols were based on the same set of algorithms that use distance vectors to mathematically compare routes to identify the best path to any given destination address. These algorithms emerged from academic research that dates back to 1957.

Today's open standard version of RIP, sometimes referred to as IP RIP, is formally defined in two documents: Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became both more numerous and greater in size, it became apparent to the Internet Engineering Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388 in January 1993, which was then superceded in November 1994 by RFC 1723, which describes RIP 2 (the second version of RIP). These RFCs described an extension of RIP's capabilities but did not attempt to obsolete the previous version of RIP. RIP 2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure table updates.

Any host that uses RIP is assumed to have interfaces to one or more networks. These are referred to as its “directly-connected networks”. The protocol relies on access to certain information about each of these networks.

There are different types of RIP packets. (Explaining the processing of IP datagrams and fragments is beyond the scope of this document.) RIPv2 enables RIP messages to carry more information, which permits the use of a simple authentication mechanism to secure table updates. More importantly, RIPv2 supports subnet masks, a critical feature that was not available in RIPv1.

8.5 CONFIGURING RIP

The following describes configuration steps for RIP.

By default, RIP is disabled. Virtual Router (VR) is currently not supported; thus there is only one instance of RIP running at one time on a <NetSecure 6100>.

This section describes the following basic steps to configure RIP on a <NetSecure 6100>:

- Enable the RIP instance globally.
- Enable RIP on interfaces that connect to other RIP routers.
- Configure remote RIP neighbors across IPSec tunnels.
- Redistribute routes learned from different routing protocols (such as OSPF, BGP, or statically configured routes) into the RIP instance.

You can also optionally configure other RIP parameters such as the following:

- Global parameters, such as timers and trusted RIP neighbors, which are set at the global level for the RIP protocol
- Interface parameters, such as neighbor authentication, which are set on a per-interface basis for the RIP protocol
- Security-related RIP parameters, which are set at either the global level or on a per-interface basis (see ‘Security Configuration’)

8.6 ENABLING AND DISABLING RIP ON INTERFACES

By default, RIP is disabled on all interfaces and you must explicitly enable it on an interface. When you disable RIP at the interface level, RIP does not transmit or receive packets on the specified interface. Interface configuration parameters are preserved when you disable RIP on an interface. To enable RIP on an interface, enter:

set interface name protocol rip enable

To disable RIP on an interface, enter:

unset interface name protocol rip

GUI Example: To globally enable RIP

- Network > Routing > RIP
- Enter the following RIP information then click **Apply**:
  Select Enable RIP option

GUI Example: Reject default route leadrned by RIP

- Network > Routing > RIP
- Enter the following RIP information then click **Apply**:
  Select Reject Default Route Learned by RIP

GUI Example: Disable advertise default route

- Network > Routing > RIP
- Enter the following RIP information then Click **Apply**:
  Uncheck the Advertise Default route

8.7 DISABLE ROUTE SUMMARIZATION

By default, RIPv2 supports automatic route summarization. The software summarizes subprefixes to the classful network boundary when crossing classful network boundaries. If you have disconnected subnets, you should disable automatic route summarization to advertise the subnets. (When route summarization is disabled, the software transmits subnet and host routing information across classful network boundaries.) To disable automatic summarization (which is enabled by default), use the following command, in router configuration mode:

set router rip auto-summary disable

8.8 ENABLE OR DISABLE SPLIT HORIZON

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router to any interface from which that information originated. This behavior usually optimizes communication among multiple routers, particularly when links are broken. However, with non-broadcast networks (such as Frame Relay and SMDS), situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon. This applies to IGRP and RIP.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

8.9 ENABLE RIP AUTHENTICATION

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface.

The <NetSecure 6100> VPN/Firewall supports two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is none.

8.10 ACCEPTING PACKETS WITH NON -ZERO RESERVED FIELDS

Some of the reserved fields in RIP version 1 packets must be zero, while in RIP version 2 packets, most of these reserved fields can contain nonzero values. By default, RIP discards version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements RIP v1/2 specifications.

Chapter 9. Policy Configuration

This chapter describes how to create and apply security policies. This chapter includes the following topics:

- About Security Policies
- Configuring Policies
- Configuring Address Objects
- Configuring Service Objects
- Configuring Service Groups
- About Schedules

9.1 ABOUT SECURITY POLICIES

A policy allows, denies, or rejects specific traffic based on the source, destination, and service type sent in a single direction between two end points. The unidirectional nature of policies requires that two policies are configured for traffic that is initiated from either side of two end points.

9.1.1 ABOUT TRAFFIC FLOW AMONG POLICIES

The default behavior of the appliance is to deny traffic from one zone to another. To permit communication from one zone to another, you must configure a policy. After you use the **set policy** command to create a policy, the policy enters the policy database and is immediately active.

The source zone, destination zone, and order of a policy within the database are important. The <NetSecure 6100> software assigns each policy an ID number

which numerically orders all policies in ascending order. Incoming traffic is first determined to be interzone or intrazone using the source and destination zone information. It is then matched against policies in the database from top to bottom.

If the source and destination zones are different, then the interzone policies are searched for a matching policy. If there is no match, then the global policies are searched. If there is no match, a default zone policy is applied and the packet is dropped. If the source and destination zones are the same, then the CARD2-G software searches intrazone policies first. If there is no match, then the software searches global policies. If there is still no match, the software applies a default zone policy that drops the packet.

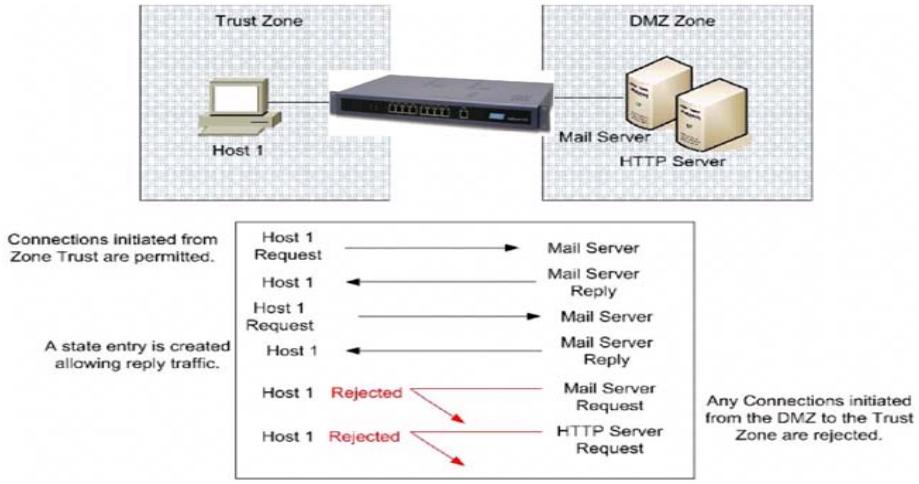


Figure 9-1 Display the use of security policies

9.1.2 ABOUT SECURITY POLICY TYPES

You can configure three types of policies for the appliance:

- Interzone Policy. Refer to Configuring Interzone Policies.
- Intrazone Policies. Refer to Configuring Intrazone Policies.
- Global Policies. Refer to Configuring Global Policies.

9.1.2.1 CONFIGURING INTERZONE POLICIES

An interzone policy controls traffic between zones. These policies can allow, deny,

or reject traffic that is to pass from one zone and destined for another. For example, in Figure 9-2, the appliance is configured with a policy that allows HTTP traffic initiated from Host A in the trust zone to Server B in the untrust zone using the following command:

- set policy from trust to untrust Host_A Server_B http permit
- save

If Server B initiates an HTTP connection, the appliance drops the packet, since no configured policy allows any HTTP requests from the untrust zone to the trust zone.

Figure 9-2: Interzone Policy

Figure 9-2 Interzone Policy

9.1.2.2 CONFIGURING INTRAZONE POLICIES

Intrazone policies control traffic to and from all hosts within the same zone. By default, all hosts configured in the same zone can communicate. Therefore, a policy allowing communication between hosts within a zone is unnecessary. In Figure 9-3, intrazone blocking is enabled to restrict hosts from communicating with each other. Intrazone blocking denies all traffic between two or more subnets configured to be in the same zone.

Use the **set zone** command with the **block** option to block intrazone communication:

set zone {name_str} block

[NOTE] Intrazone blocking is disabled by default. All communication among hosts on a zone is allowed.

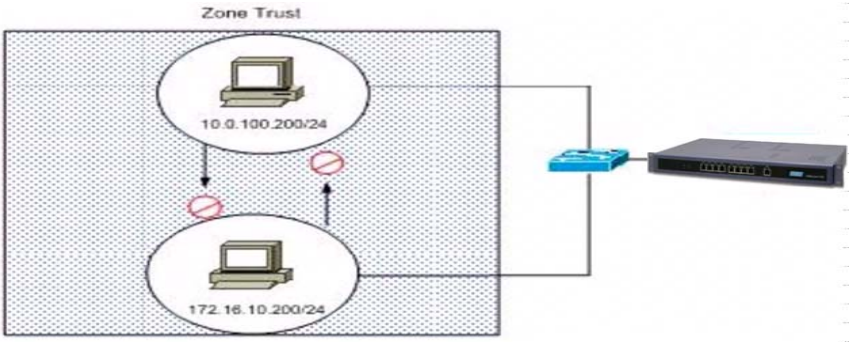


Figure 9-3 Intrazone Policy

9.1.2.3 CONFIGURING GLOBAL POLICIES

Global policies are not assigned to a specific zone and either allow or deny packets to all zones.

Use the **set zone** command and specify **global** as the zone to create a global policy:

- set policy global {src_addr} {dst_addr} {srvc} {permit | deny | reject}

[NOTE] You must configure the src_addr and dst_addr in the global zone.

9.2 CONFIGURING POLICIES

This section describes how to create, modify and delete policies. This section includes the following topics:

- Creating Policies
- Naming Policies
- Reordering Polices
- Disabling Policies
- Re-enabling Policies
- Deleting Policies
- Viewing Policies

9.2.1 CREATING POLICIES

The service type, location of end points, and policy action are the primary elements of a policy.

Use the **set policy** command to create a policy:

set policy from {src_zone} to {dst_zone} {src_addr} {dst_addr} {srvc} {permit | deny | reject | tunnel}

Table 9-1 explains the parameters in the above command.

Table 9-1: Addresses and Zones

Parameter	Description
{src_zone}, {dst_zone}	The **{src_zone}** and **{dst_zone}** objects are used to define the direction of the policy and whether the traffic is interzone or intrazone.

{src_addr}, {dst_addr}	The **{src_addr}** and **{dst_addr}** are source and destination address objects. This information is also used for route lookups determining the ingress and egress interface of the policy.
{srvc}	The **{srvc}** object defines the destination port for the traffic.
permit	The **permit** action allows traffic matching the policy to pass through.
deny	The **deny** action drops traffic matching the policy.
reject	The **reject** action sends a TCP reset to the transmitter.
tunnel	The **tunnel** action allows the encryption (using IPsec) of traffic that matches the policy.

Refer to the following related topics:

- Naming Policies—Creating a name or alias to the refer to the policy.
- Enable Policy Logging—Turning policy logging on or off.
- About Schedules—Adding day and time schedules for the policy.

Example: Create a policy

Allow FTP traffic from the eth1 interface in the untrust zone to a server with IP address 4.4.4.4 on the eth0 interface in the trust zone:

- set address trust FTPtrust 4.4.4.4
- set policy from untrust to trust any FTPtrust ftp permit
- save

GUI Example: Create a policy

- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: FTP Trust
  IP Address/Netmask: 4.4.4.4/24
  Zone: Trust
- Policy > Add Policy

- Enter the following, then click **Apply**:
  Location
  Action: Permit
  Source Zone: Untrust
  Destination Zone: Trust
  Source Address: Any
  Destination Address: FTPTrust
  Service: FTP

9.2.2 NAMING POLICIES

Use the **set policy** command with the **name** option to add a name when you create the policy:

set policy name {name_str} from {src_zone} to {dst_zone} {src_addr} {dst_addr} {srvc} permit | deny | reject

Use the set policy command with the name option to add a name to an existing policy:

set policy id {number} name {name} from {src_zone} to {dst_zone} {src_addr} {dst_addr} {srvc} permit | deny | reject

Example: Adding a name to the policy from the previous example.

- set policy id 1 name ftpcorp from untrust to trust any 4.4.4.4 ftp permit
- save

GUI Example: Adding a name to the policy from the previous example.

- Policy > Configuration Edit
- Enter the following, then click **Apply**.
  Enable Policy
  Name: ftpcorp
  Action: permit
  Source Zone: untrust
  Destination Zone: trust
  Source Address: any
  Destination: 4.4.4.4
  Service: FTP

9.2.3 REORDERING POLICES

Because the policy database is searched from top to bottom when matching against traffic, you should order polices in the database from most specific to least specific. Doing this ensures that a more general policy does not block a more specific policy as illustrated by the policy example below. In this example, policy 2 never matches against FTP requests initiated from the trust zone to a server on the untrust zone because the deny policy follows a more general allow policy.

Example: Reordering policies

Set policy id 2 from trust to untrust any any ftp deny

GUI Example: Reordering policies

- Policy > Configuration > Edit (for ID1)
- Enter the following, then click **Apply**:
  Location
  Action: Permit
  Source Address: Any
  Destination Address: Any
  Service: Any
- Policy > Configuration > Edit (for ID2)
- Enter the following, then click **Apply**:
  Location
  Action: Deny
  Source Address: Any
  Destination Address: Any
  Service: FTP

By default, the <NetSecure 6100> software assigns a newly created policy a policy ID and adds it to the bottom of the policy list. To restrict FTP traffic from trust to untrust Policy 2 reordered in front of Policy 1.

Use the set policy command with the move option to re-order policies in the policy database:

set policy move {id_num} { before | after } {target_id}

The *{id_num}* number specifies the policy number that is moved; the *{target_id}* is the policy number that the policy is moved before or after.

9.2.4 DISABLING POLICIES

Use the **set policy** command with the **disable** option to disable a policy rather that delete it from the policy database:

set policy id {id_num} disable

9.2.5 RE-ENABLING POLICIES

Use the **unset policy** command with the **disable** option to enable a policy that has been set to disable:

unset policy id {id_num} disable

9.2.6 DELETING POLICIES

Use the **unset policy** command with the **id** option to delete a policy by specifying a policy number:

unset policy id {number}

9.2.7 VIEWING POLICIES

You can display policies using the **get policy** command:

get policy

This displays all policies in the policy database (with the exception of global policy) in table format. The table appears with the following columns:

- ID
- From
- To
- Src-address
- Dst-address
- Service
- Action
- State

Use the **get policy** command with the **all** option to display all policies in the policy database including global policies in table format:

get policy all

The table appears with these columns:

- ID
- From
- To
- Src-address
- Dst-address
- Service
- Action
- State

Use the **get policy** command with the **id** option to display a specific policy:

get policy id {number}

This command returns the following information about the policy with the specified ID number:

- get policy id 202

- ID: 202
- Name:
- Action: permit
- Status: enabled
- From: trust
- To: trust
- Src: any
- Dst: any
- Service: any
- NAT: off
- Schedule: N/A

Use the **get policy** command with **from** or **to** option to display all policies that match the **src_zone** and **dst_zone** parameters in table format:

get policy from {src_zone} to {dst_zone}

The table appears with the following columns:

- ID
- From
- To
- Src-address
- Dst-address
- Service
- Action
- State

Use the **get policy** command with the **global** option to display all global policies in the policy database in table format:

get policy global

The table appears with these columns.

- ID
- From
- To
- Src-address
- Dst-address
- Service
- Action
- State

9.2.8 ENABLE POLICY LOGGING

By default, logging per policy is disabled. To enable policy logging use the **set policy** command with the **log** option:

set policy from {src_zone} to {dst_zone} {src_addr} {dst_addr} {srvc} permit | deny | reject

For additional information about logging refer to Chapter 1 Overview.

9.3 CONFIGURING ADDRESS OBJECTS

Before you can configure any policies to deny or permit access to or from a host or network, you must create address objects and assign them to a zone. These objects can be a single host, a subnet or a group of multiple address objects.

This section describes how to create, modify and delete address objects. The following topics are included in this section:

- Creating Address Objects
- Deleting Address Objects
- Modifying Address Objects
- Creating Address Groups
- Adding Objects to an Address Group
- Deleting Address Groups
- Adding Comments to Address Groups

9.3.1 CREATING ADDRESS OBJECTS

All address objects bind to a security zone specified during creation.

Use the **set address** command to create host objects or subnet objects which are defined by an IP address and subnet mask:

set address {zone} {name_str} {ip_addr/mask}

[NOTE] The pre-defined address object any refers to all hosts in that zone.

Example: Creating an address object

Figure 9-4: Address Objects

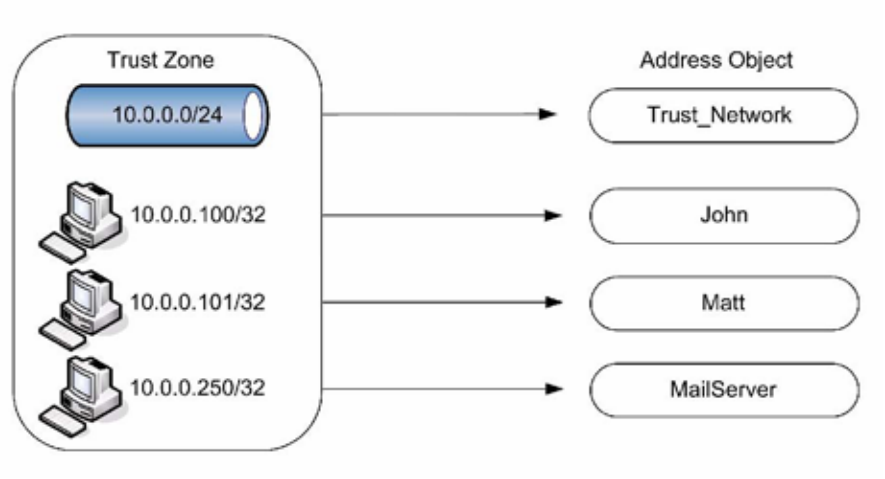


Figure 9-4 Address Objects

To create the address objects shown in Figure 9-4:

- Create an address object for the IP address 10.0.0.100 using the name John.
- Create an address object for the IP address 10.0.0.101 using the name Matt.
- Create an address object for the IP address 10.0.0.250 using the name MailServer.
- Create an address object for the subnet 10.0.0.0/24 using the name Trust_Network.
  - set address trust John 10.0.0.100/32
  - set address trust Matt 10.0.0.101/32
  - set address trust MailServer 10.0.0.250/32
  - set address trust Trust_Network 10.0.0.0/24
  - save

GUI Example: Creating an address object

- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: John
  IP Address/Netmask: 10.0.0.100/32
  Zone: Trust

- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: Matt
  IP Address/Netmask: 10.0.0.101/32
  Zone: Trust
- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: MailServer
  IP Address/Netmask: 10.0.0.250/32
  Zone: Trust
- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: Trust_Network
  IP Address/Netmask: 10.0.0.0/24
  Zone: Trust

9.3.2 DELETING ADDRESS OBJECTS

Use the **unset address** command to delete an address object:

unset address {zone} {name_str}

9.3.3 MODIFYING ADDRESS OBJECTS

To modify the name, IP address. or subnet mask of an existing address object, first delete the object, then re-create the object with the new settings.

Example: Modify an address object

Change the name of the address object from *MailServer* to *MailServerNY*:

- unset address trust MailServer
- set address trust MailServerNY 10.200.0.0/24

- save

GUI Example: Modify an address object

- Objects > Address Objects
- Select the following, then click **Apply**:
  Remove: MailServer
- Objects > Add Address Objects
- Enter the following, then click **Apply**:
  Name: MailServerNY
  IP Address/Netmask: 10.200.0.0/24
  Zone: Trust

Use the **get address** command to view all address objects and address groups:

```
get address
```

The command displays all objects grouped by their zone membership.

Use the **get address** command and specify a zone to view all address objects and address groups in that zone:

```
get address {zone}
```

Use the **get address** command and specify the zone and object name to view the address object by name:

```
get address {zone} name {adr_obj}
```

9.3.4 CREATING ADDRESS GROUPS

Address groups include multiple address objects. Use the **set group** command with the **address** option to create an address group:

```
set group address {zone} {grp_name}
```

9.3.5 DDING OBJECTS TO AN ADDRESS GROUP

Use the **set group** command with the address and **add** options to add an address object to an address group:

set group address {zone} {grp_name} add {adr_obj}

The following limitations apply to address groups:

- Address groups cannot have the same name as an address object.
- If the policy database references an address group, you cannot delete the address group until you first remove it from the policy database.
- One address group cannot have another address group as a member.

Example: Creating an address group

Figure 9-5: Address Groups

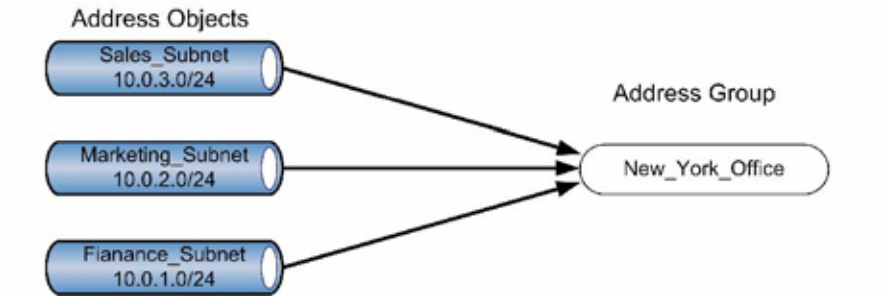


Figure 9-5 Address Groups

To create the address objects and address group in Figure 9-5, follow these steps:

- set address trust Finance_Subnet 10.0.1.0/24
- set address trust Mktg_Subnet 10.0.2.0/24
- set address trust Sales_Subnet 10.0.3.0/24
- set group address trust New_York_Office
- set group address trust New_York_Office add Finance_Subnet
- set group address trust New_York_Office add Mktg_Subnet

- set group address trust New_York_Office add Sales_Subnet
- save

GUI Example: Creating an address group

- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: Finance_Subnet
  IP Address/Netmask: 10.0.1.0/24
  Zone: Trust
- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: Mktg_Subnet
  IP Address/Netmask: 10.0.2.0/24
  Zone: Trust
- Objects > Add Address Object
- Enter the following, then click **Apply**:
  Name: Sales_Subnet
  IP Address/Netmask: 10.0.3.0/24
  Zone: Trust
- Objects > Add Address Group
- Enter the following, then click **Apply**:
  Name: New_York_Office
  Zone: Trust
  Go
  Add: Fianace_Subnet, Mtkg_Subnet, and Sales_Subnet

9.3.6 DELETING ADDRESS GROUPS

Use the **unset group** command with the **address** option to delete and address group:

unset group address {zone} {grp_name}

[NOTE] You cannot delete the group if it is bound to a policy.

9.3.7 DELETING ADDRESS OBJECTS FROM AN ADDRESS GROUP

Use the **unset group** command with the **address** and **remove** options to remove an address object from an address group:

unset group address {zone} {grp_name} remove {adr_obj}

[NOTE] If you remove all of the address objects out of an address group, the address group name is not deleted.

9.3.8 ADDING COMMENTS TO ADDRESS GROUPS

Use the **set group** command with the **address** and **comment** options to add a comment that describes the address group:

set group address {zone} {grp_name} comment “{text}”

Example: Adding the comment “ALL DEPARTMENTS” to the group object NEW_YORK_OFFICE

- set group address trust New_York_Office comment “All Departments”
- save

GUI Example: Adding the comment “ALL DEPARTMENTS” to the group object NEW_YORK_OFFICE

- Objects > Address Groups
- Enter the following, then click **Apply**:
  Zone: Trust
  Go
  Edit: New_York_Office
  Comment: All_Departments

9.4 CONFIGURING SERVICE OBJECTS

Service objects used in policies consist of a transport protocol and an associated port number. For example, FTP is associated with protocol TCP and port number 21; HTTP is TCP/port 80, and SSL is TCP/port 443. You can select service objects from a predefined list or you can create a custom service object.

This section describes how to create, modify and delete address objects. The following topics are included in this section:

- Viewing Predefined Service Objects
- Configuring Custom Service Objects
- Deleting Service Objects
- Modifying Service Objects
- Configuring Service Timeouts

9.4.1 VIEWING PREDEFINED SERVICE OBJECTS

To view predefined service objects, use the **get service** command:

```
get service pre-defined
```

For a list of predefined services, refer to Appendix , “Pre-defined Services.”

9.4.2 CONFIGURING CUSTOM SERVICE OBJECTS

Use the **set service** command with the **name**, **protocol**, **src-port** and **dst-port** options to create a custom service object:

```
set service {name_str} protocol {prot_type} [ src-port {range} ] dst-port {range}
```

Example: Adding a custom service object

- set service custom protocol tcp src-port 1-65535 dst-port 23005-23005
- save

GUI Example: Adding a custom service object

- Objects > Add Custom Service
- Enter the following, then click **Apply**:
  Name: telnet_custom
  TCP
  Source Port Low: 1
  Source Port High: 65535
  Destination Port Low: 23005
  Destination Port Low: 23005

9.4.3 DELETING SERVICE OBJECTS

Use the **unset** command to delete an existing service object:

- unset service {name_str}

9.4.4 MODIFYING SERVICE OBJECTS

To modify the values of an existing service object, first delete the object, and then re-create the object with the new settings.

Example: Modifying a custom service

Change the destination port on Telnet_Custom to port 24000:

- unset service Telnet_Custom
- set service Telnet_Custom protocol tcp src-port 1-65535 dst-port 24000-24000
- save

GUI Example: Modifying a custom service

- Objects > Custom Service
- Select the following, then click **Apply**:
  Remove: telnet_custom
- Objects > Add Custom Service
- Enter the following, then click **Apply**:
  Name: telnet_custom
  TCP
  Source Port Low: 1
  Source Port High: 65535
  Destination Port Low: 24000
  Destination Port Low: 24000

9.4.5 CONFIGURING SERVICE TIMEOUTS

Set the threshold timeout (in minutes) for a predefined service or custom service using the **set service** command with the **timeout** option:

set service {name_str} timeout {minutes}

Use the default service timeout (5 minutes) or specify a new threshold

Example: Changing a service TIMEOUT

Increase the timeout on the predefined service FTP from 5 minutes to 15 minutes:

- set service ftp timeout 15
- save

You can use the following options to define the additional properties of the service:

- Code Values and Type for ICMP Services
- Timeout Value

9.5 CONFIGURING SERVICE GROUPS

You can use service groups to select a set of service objects and put them into group using a single name. After you add service objects to a service group, you can apply the services to a security policy, thus simplifying administration. A service group can consist of pre-defined services or custom services.

Service groups have the following limitations:

- Service groups cannot have the same name as a pre-defined or custom service.
- You cannot delete a service group until you first remove it from the policy.
- A service group cannot have another service group as a member.
- The all-inclusive service term “ANY” cannot be added to groups.

This section describes how to create, modify and delete service groups. The following topics are included in this section:

- Creating Service Groups
- Deleting Service Groups
- Deleting Service Objects
- Modifying Service Groups
- Adding Comments to Service Groups

9.5.1 CREATING SERVICE GROUPS

Use the **set group** command with the **service** option to create a service group:

set group service {name_str}

Use the **set group** command with the **service** and **add** options to add service objects to a service group:

set group service {name_str} add {service_object}

Example: Changing a service TIMEOUT

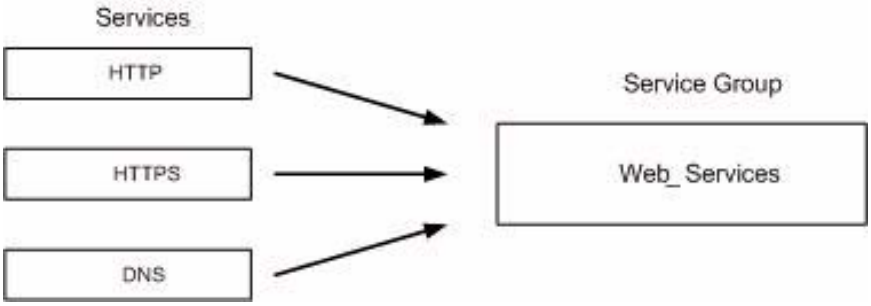


Figure 9-6 Service Groups

Use the following commands to create a service group called Web_Service as displayed in Figure 9-6:

- set group service Web_Services
- set group service Web_Services add http
- set group service Web_Services add https
- set group service Web_Services add dns
- save

GUI Example: Changing a service TIMEOUT

- Objects > Add Service Group
- Enter the following, then click **Apply**:
  Name: Web_Services
  Add: http, https, dns

9.5.2 DELETING SERVICE GROUPS

Use the **unset group** command with the **service** option to delete a service group:

unset group service {name_str}

9.5.3 REMOVING SERVICE OBJECTS FROM GROUPS

Use the **unset group** command with the **service** and **remove** options to remove a specific service from the group.:

unset group service {name_str} remove {name_str}

To remove all services in the group, use the **clear** option.

9.5.4 MODIFYING SERVICE GROUPS

To modify a service group, you must first remove the service group and all of the service objects. Then add the group again with those service objects you want to include.

Example: Modifying a service group

Modify the service group Web Services to add HTTP and DNS:

- unset group service Web_Services
- set group service Web_Services add http
- set group service Web_Services add dns
- save

GUI Example: Modifying a service group

- Objects > Service Groups
- Enter the following, then click **Apply**:
  Remove: Web_Services
- 3Objects > Add Service Group
- Enter the following, then click **Apply**:
  Name: Web_Services
  Add: http, and dns

9.5.5 ADDING COMMENTS TO SERVICE GROUPS

Use the **set group** command with the **service** and **comment** options to add a comment that describes the address group:

set group service {grp_name} comment “{text}”

[NOTE] If you remove all of the services in a service group, that service group name is not deleted.

9.6 ABOUT SCHEDULES

A schedule is an object that defines the day and time a policy is action takes place.

This section describes how to create, add, view and delete schedules. The following topics are included in this section:

- Creating One-time Schedules
- Creating Recurring Schedules
- Adding Schedules to Policies
- Deleting Schedules
- Viewing Schedules

9.6.1 CREATING ONE -TIME SCHEDULES

[NOTE] Schedules must have minimum start and stop times of at least five minutes.

Use the **set scheduler** command with the **once** option to create a schedule object for a one time event:

set scheduler {name} once start {date} {time} stop {date} {time} comment {text}

Table 9-2 explains the parameters in the above command.

Table 9-2 One-time Schedule

Parameter	Description
{name}	The **{name}** field assigns a name to the schedule. Schedules are assigned to policies by referring to the schedule name.
once	The **once** option is used to define a one time event.
start	Use the **start** option and specify a day and time to allow traffic matching the policy to pass through.
stop	Use the **stop** option and specify a day and time stop traffic matching the policy to pass through.
{date}	The **{date}** field requires an mm/dd/yyyy format.
{time}	The **{time}** field requires an hh:mm format.
comment	Use the **comment** command to add a comment associated with the schedule.
{text}	The **{text}** field is a line of text.

9.6.2 CREATING RECURRING SCHEDULES

Use the **set schedule**r command with the **recurrent** option to create a schedule object for a recurring event:

set scheduler {name} recurrent {day} start {time} stop {time} comment {text}

Table 9-3 explains the parameters in the above command.

Table 9-3 Recurring Schedule

Parameter	Description
{name}	The **{name}** field assigns a name to the schedule. Schedules are assigned to policies by referring to the schedule name.
recurrent	The **recurrent** option is used to define a recurring event.
{day}	The **{day}** field requires an mm/dd/yyyy format.
start	Use the **start** option and specify a time to allow traffic matching the policy to pass through.
stop	Use the **stop** option and specify a time stop traffic matching the policy to pass through.

Parameter	Description
{day}	The **{day}** field is a day of the week. The list choices are: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday
{time}	The **{time}** field requires an hh:mm format.
comment	Use the **comment** command to add a comment associated with the schedule.
{text}	The **{text}** field is a line of text.

A recurrent schedule can accept two sets of start/stop commands. You can use these commands for schedules that are enabled or disabled throughout the day with the exception of a specific period of time:

set scheduler {name} recurrent {day} start {time} stop {time} start {time} stop {time}

Specify the same schedule name in multiple **set scheduler** commands to add additional days to the same schedule.

9.6.3 ADDING SCHEDULES TO POLICIES

Use the **set policy** command with the **schedule** option to add a schedule to a policy:

set policy from {zone} to {zone} {src_adr} {dst_adr} {srvc} schedule {name_str}

Example: Create a recurring schedule

Create a recurring schedule to block Internet access on the weekend for all machines on the trust zone:

- set scheduler “weekend” recurrent sunday start 00:00 stop 23:59 comment “Block weekend Internet access”
- set scheduler “weekend” recurrent saturday start 00:00 stop 23:59 comment “Block weekend Internet access”
- set policy from trust to untrust any any any deny schedule weekend

- save

GUI Example: Create a recurring schedule

- Objects > Add Schedule
- Enter the following, then click **Apply**:
  Name: weekend
  Comment: Block weekend Internet access
  Recurring
  Sunday start: 00:00
  Sunday end: 23:59
  Saturday start: 00:00
  Saturday end: 23:59
- Policy > Add Policy
- Enter the following, then click **Apply**:
  Location
  Action: Deny
  Source Zone: Trust
  Destination Zone: Untrust
  Source Address: any
  Destination Address: any
  Service: any
  Schedule: weekend

9.6.4 DELETING SCHEDULES

To delete a schedule, use the **unset scheduler** command:

unset scheduler {name_str}

9.6.5 VIEWING SCHEDULES

Use the **get scheduler** command with the **once**, **recurrent** or **name** options to view all configured schedules:

- get scheduler once

- get scheduler recurrent
- get scheduler {name_str}

Chapter 10. Address Translation

This chapter describes the different methods of address translation that you can enable for traffic passing through the appliance. This chapter includes the following topics:

- Network Address Translation
- Configuring Source Network Address Translation
- Source NAT Configurations
- Configuring Destination NAT and Port Mapping
- Destination NAT Configurations

10.1 NETWORK ADDRESS TRANSLATION

Enabling Network Address Translation (NAT) on traffic passing through the appliance modifies the IP address in the IP packet header. Optionally, enabling NAT also modifies the port number in the transmission control protocol (TCP) segment or user datagram protocol (UDP) datagram. You can enable NAT either on the interface or through the security policy database. This chapter describes how to enable NAT through the security policy database. For information on enabling NAT on the interface, refer to Chapter 3 Security Zone and Interfaces.

There are four primary NAT configurations:

- **One-to-one NAT**—Enables translation of a single public IP address into a private IP address. One-to-one NAT is often used to allow a host on a private network to be accessed from the Internet.
- **Many-to-one NAT**—Enables translation of multiple private IP addresses into a single public IP address, allowing all hosts on the private network to access the Internet as a single entity.

- **Many-to-many NAT**—Enables translation of multiple private IP addresses into multiple public IP addresses. The length of defined ranges need not match.
- **Port Address Translation (PAT)**—Enables translations of the original source port number to a different, randomly assigned port number.

10.2 CONFIGURING SOURCE NETWORK ADDRESS TRANSLATION

When performing source NAT, the policy translates the source IP address to a different address. The source IP address is either translated to a single address or to an address randomly chosen from a pool of addresses defined in a dynamic IP (DIP) pool. Figure 10-1 displays an example of source IP address translation.

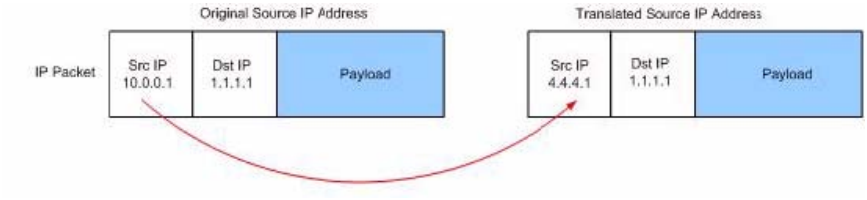


Figure 10-1 Source IP Address Translation

Use the **set policy** command with the **nat src** option to specify source NAT in the policy.

set policy from {zone} to {zone} {src_ad} (dst_ad) {srvc} nat src permit

If you configure the policy without specifying a DIP pool ID, the policy uses the source address of the egress interface as the translated address

Use the **set policy** command with the **nat src** and **dip-id** options to specify the source NAT to use a random address from the DIP pool:

set policy from {zone} to {zone} {src_ad} {dst_ad} {srvc} nat src dip-id {id} permit

10.2.1 ABOUT PORT ADDRESS TRANSLATION (PAT)

PAT translates the original source port to a random source port to maintain the uniqueness of all outbound connections. After an outbound connection is made, the <NetSecure 6100> software enters the combination of the translated source IP address, translated source port, and destination IP address in the session table. As more hosts from the original source network set up connections in the session table, the entries all have the same translated source IP address, but different translated source ports.

10.2.2 CONFIGURING DYNAMIC IP (DIP) POOLS

Use dynamic IP (DIP) pools to create a pool of IP addresses to use for source NAT policies. Use the **set interface** command with the **dip** option to create a DIP pool of addresses on the egress interface:

set interface {interface name} dip {dip id} {start address} {end address}

Addresses in the DIP pool must be on the same subnet as the corresponding egress interface. You can create multiple DIP pools created, each identified with a different dip-id number.

Use the **unset interface** command with the **dip** option to delete a DIP pool from the interface:

unset interface {interface name} dip {dip id}

10.3 SOURCE NAT CONFIGURATIONS

This section describes two types of source NAT configurations that you can use with this appliance:

- Source NAT, or Many-to-One with Port Address Translation
- Destination NAT and Port Mapping

10.3.1 CONFIGURING SOURCE NAT: MANY-TO-ONE WITH PORT ADDRESS TRANSLATION

In a source NAT many-to-one NAT configuration, all original source IP addresses on a network translate to a single IP address (Figure 10-2).

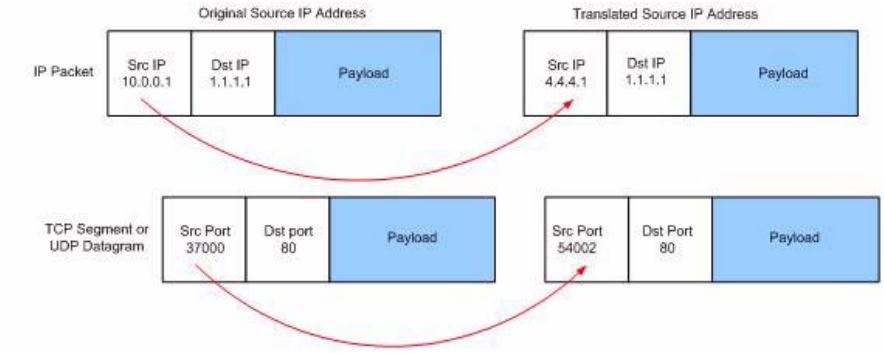


Figure 10-2 Source IP Address Translation with Port Address Translation

Use the **set policy** command with the **nat src** option to specify source NAT in the policy. In this configuration, the source address src_grp is an address group consisting of a subnet, address range, or multiple hosts.

set policy from {zone} to {zone} {src_grp} (dst_addr) {port} nat src permit

10.3.2 CONFIGURING SOURCE NAT: MANY-TO-MANY WITH PORT ADDRESS TRANSLATION

In a source NAT many-to-many NAT configuration, all source IP addresses

translate to an IP address dynamically taken from a DIP pool on the egress interface. The total number of translated addresses available in the DIP pool might be less than the number of source addresses in the source network. In this case, addresses from the DIP pool can be used multiple times for source NAT sessions. PAT is then used to ensure each outgoing session is unique in the session table.

Use the **set policy** command with the **nat src** and **dip-id** options to specify source NAT in the policy.

set policy from {zone} to {zone} {src_grp} {dst_addr} {port} nat src dip-id {id} permit

In this configuration, the source address src_grp is an address group consisting of a subnet, address range or multiple hosts:

10.4 CONFIGURING DESTINATION NAT AND PORT MAPPING

Destination NAT can translate a single destination address to a single address (one-to-one), translate one range of destination addresses to a single address (many-to-one) or translate one range of destination addresses to another range of addresses (many-to-many) (refer to Figure 10-3).

Port mapping increases the number of services supported for a single address by changing the destination port in one-to-one NAT and many-to-one NAT configurations. Unlike port address translation, which randomly assigns the port during translation, port mapping uses a policy-assigned port.

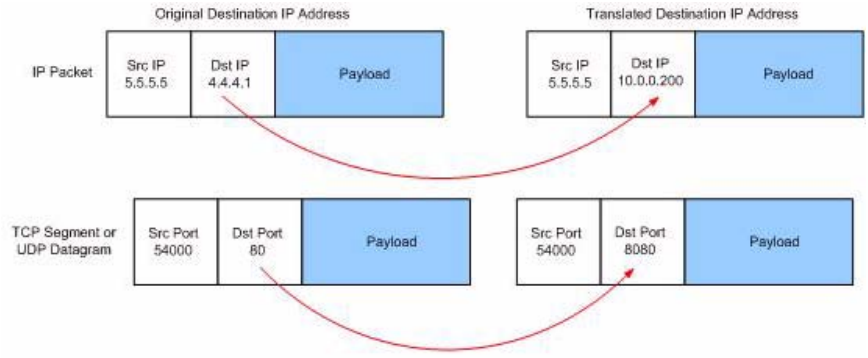


Figure 10-3 Destination NAT with Port Mapping

Use the **set policy** command with the **nat dst ip** and **port** options to specify destination NAT and port mapping in the policy:

set policy from {zone} to {zone} {src_addr} (dst_addr) {srvc} nat dst ip {nat_addr} port {prt_nbr} permit

10.5 DESTINATION NAT CONFIGURATIONS

This section describes in detail the types of destination NAT configurations you can use with the appliance. This section includes the following topics:

- Configuring Destination NAT: One-to-One
- Configuring Destination NAT: One-to-One with Port Mapping
- Configuring Destination NAT: Many-to-One
- Configuring Destination NAT: Many-to-One with Port Mapping
- Configuring Destination NAT: Many-to-Many

10.5.1 CONFIGURING DESTINATION NAT: ONE-TO-ONE

In a one-to-one destination NAT configuration, a single destination address translates to a different address that the security policy specifies (refer to Figure 10-4). The most common use for one-to-one NAT is to allow hosts on the Internet to access hosts on a Demilitarized Zone (DMZ).

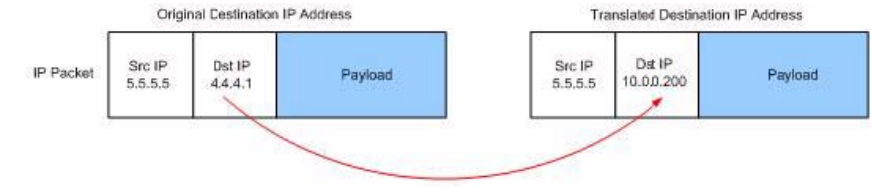


Figure 10-4 Destination Network Address Translation

Use the **set policy** command with the **nat dst ip** option to specify destination NAT in the policy:

set policy from {zone} to {zone} {src_addr} (dst_addr) {port} nat dst ip {nat_addr} permit

10.5.2 CONFIGURING DESTINATION NAT: ONE-TO-ONE WITH PORT MAPPING

Use the **set policy** command with the **nat dst ip** and **port** options to specify destination NAT from a single address and port to a single address and port:

set policy from {zone} to {zone} {src_addr} (dst_addr) {port} nat dst ip {nat_addr} port {prt_nbr} permit

10.5.3 CONFIGURING DESTINATION NAT: MANY-TO-ONE

In a many-to-one destination NAT configuration, a group of destination addresses translates to a single address that the policy specifies. Use the **set policy** command with the **nat dst ip** option to specify destination NAT in the policy. In this configuration, the destination address dst_grp is an address group consisting of a subnet, address range, or multiple hosts.

set policy from {zone} to {zone} {src_addr} (dst_grp) {port} nat dst ip {nat_addr} permit

10.5.4 CONFIGURING DESTINATION NAT: MANY-TO-ONE WITH PORT MAPPING

Use the **set policy** command with the **nat dst ip** and **port** options to specify destination NAT from an address group and port to a single address and port:

set policy from {zone} to {zone} {src_addr} (dst_addr) {port} nat dst ip {nat_addr} port {prt_nbr} permit

10.5.5 CONFIGURING DESTINATION NAT: MANY-TO-MANY

Use the **set policy** command with the **nat dst ip** option to specify destination NAT that translates a group of destination addresses to an address from a specified address range:

set policy from {zone} to {zone} {src_addr} (dst_grp) {port} nat dst ip {nat_addr_begin} {nat_addr_end} permit

The NAT address range is specified by **nat_addr_begin** and **nat_addr_end**.

Destination NAT in a many-to-many configuration employs address shifting to translate the first destination address in an address range to the first address from the destination NAT range. The translated addresses maintain consistency. Refer to Figure 10-5 for an example.

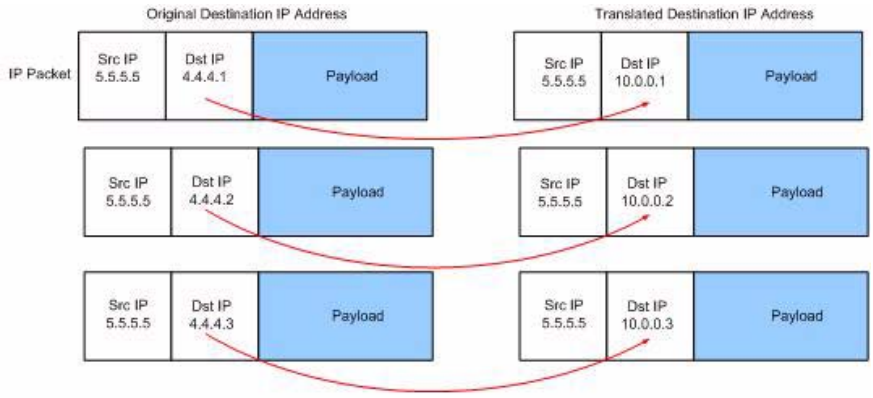


Figure 10-5 Destination Network Address Translation with Address Shifting

Chapter 11. High Availability

This chapter describes the High Availability feature. It includes the following topics:

- About High Availability
- Software Architecture overview
- CLI Commands
- HA Configuration

11.1 ABOUT HIGH AVAILABILITY

High Availability (HA) provides continuous service to end users when link and/or node failures occur. HA functionality interfaces with almost all subsystems of the product.

HA functionality includes three interacting state machines to provide heartbeat, election, and synchronization functions. Synchronization is accomplished over a TCP session using a custom protocol to synchronize configuration data between the two nodes.

11.2 SOFTWARE ARCHITECTURE OVERVIEW

Figure 11-1 illustrates the high-level view of a two node redundant system to synchronize state information between the nodes.

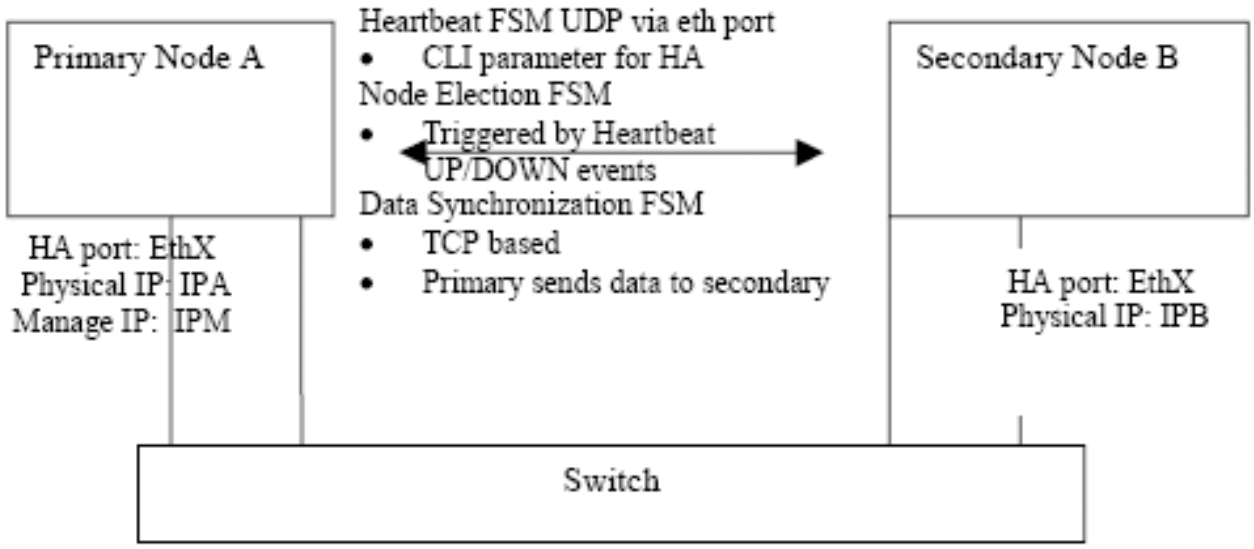


Figure 11-1 High Availability Functionality Implemented through Custom Finite State Machines (FSM)

11.3 CLI COMMANDS

Following is a partial list of supported HA commands. For more complete information on these commands, see the *CLI Reference Guide*.

Command	Description
get ha link	Displays HA link information.
set/unset ha config sync	Enables or disables synchronization between members of the vsd group.
set ha preempt	Used to preempt the primary node and take over the role of primary node.
set ha priority...	Sets HA parameters.
set ha interface...	Sets interface parameters.

11.4 HA CONFIGURATION

11.4.1 CONFIGURING THE PRIMARY AND SECONDARY IP ADDRESSES FOR THE INTERFACE

[NOTE] eth0 is the LAN side and eth1 is the WAN side.

On Node1 (Designated primary):

- set int eth0 ip 192.168.1.1/24
- set int eth0 manage-ip 192.168.1.101/24
- set int eth1 ip 1.1.1.1/24
- set int eth1 manage-ip 1.1.1.101/24*

Similary on Node 2 (Designated secondary):

- set int eth0 ip 192.168.1.2/24
- set int eth0 manage-ip 192.168.1.102/24
- set int eth1 ip 1.1.1.2/24 *
- set int eth1 manage-ip 1.1.1.102/24 *

[NOTE] manage-ip on eth1 is only required to manage the appliance from the WAN side. If no management is required from the WAN side then only one IP Address is required on the WAN side.

On Node 1:

set ha interface eth0 wan-port eth1 peer-ip 192.168.1.102

Similarly on Node 2:

set ha interface eth0 wan-port eth1 peer-ip 192.168.1.101

GUI Example: Configuring the primary and secondary IP addresses for the

interface

- Network > Interface
- Select edit eth0 interface
- Enter the following address information then click **Apply**:
  Type eth0 IP address: 192.168.1.1
  Type eth0 Netmask: 24
  Type eth0 manage-ip: 192.168.1.101
- Network > Interface
- Select edit eth1 interface
- Enter the following address information then click **Apply**:
  Type eth1 IP address: 1.1.1.1
  type eth1 Netmask: 24
  Type eth1 manage-ip: 1.1.1.102

11.4.2 CONFIGURING HA PRIORITY (VALUES 1 TO 254)

The priority of the device sets whether the device will be primary or secondary. The number closest to 1 will be designated primary.

On Node1:

set ha priority 10 hb-interval 1000 hb-threshold 3 grat-arp 4

On Node 2:

set ha priority 20 hb-interval 1000 hb-threshold 3 grat-arp 4

- hb-interval is the heart beat interval in milliseconds and can be up to 1000
- hb-threshold is the number of unsuccessful tries before fail-over happens
- grat-arp is the number of gratuitous arps a device sends when transitioning between primary and secondary

After setting the initial parameters, HA should be enabled by running the following command on both designated primary and secondary nodes:

- set ha config sync
- get ha link

[NOTE] The get command shows HA link information.

GUI Example: Set HA interface and WAN-port for node

- HA > Configuration
- Enter the following HA information then click **Apply**:
  Select HA Interface eth0
  Select WAN-Port eth1
  Type Peer-ip: 192.168.1.102

GUI Example: HA interface and WAN-port for node 2

- HA > Configuration
- Enter the following HA information then click **Apply**
  Select HA Interface eth0
  Select WAN-Port eth1
  Type Peer-ip: 192.168.1.101

GUI Example: Set HA priority for node 1

- HA > Configuration
- Enter the following HA information then click **Apply**:
  Set HA Priority 10
  Set hb-interval 1000
  Set hb-threshold 3
  Set grat-arp 4

GUI Example: Set HA priority for node 2

- HA > Configuration
- Enter the following HA information then click **Apply**:
  Set HA Priority 20
  Set hb-interval 1000
  Set hb-threshold 3
  Set grat-arp 4

GUI Example: Set HA configuration synchronization

- HA > Config Sync
- Select the HA Configuration Synchronization button

GUI Example: Display the HA link information

- HA > Information

Chapter 12. PKI & X.509/Digital Certificates

This chapter describes the Public Key Infrastructure (PKI) and X.509/Digital Certificates feature. It includes the following topics:

- About Public Key Infrastructure and X.509/Digital Certificates
- PKI Basics
- CLI Commands

12.1 ABOUT PUBLIC KEY INFRASTRUCTURE AND X.509/DIGITAL CERTIFICATES

PKI is designed to be used with IPSec instead of PSK and Manual Key. Although complex to set-up, it provides a higher level of security. Different ways to use PKI include:

- Use of self-signed certificate
- Use a Certificate Authority
- Certificate revocation lists
- Chain validation

12.2 PKI BASICS

PKI arrangements enable users to be authenticated to each other, and to use the information in identity certificates. Users are certified by a third-party also known as a Certificate Authority.

Figure 12-1: Digital Certificate Overview

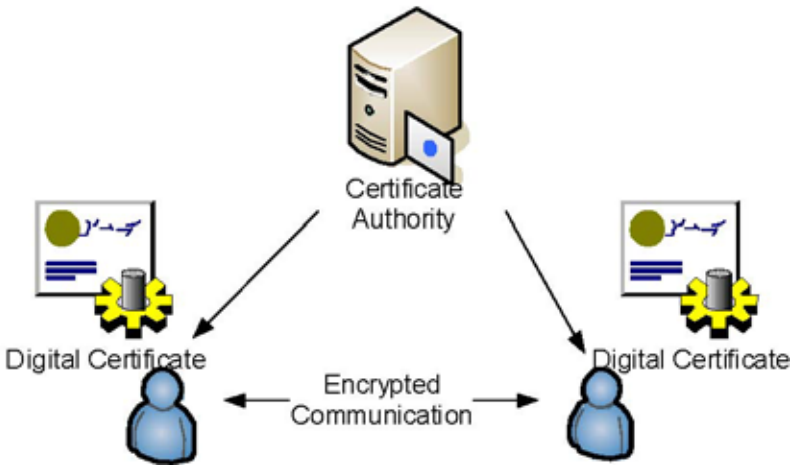


Figure 12-1 Digital Certificate Overview

12.2.1 A TYPICAL DIGITAL CERTIFICATE

The following figure shows a typical Digital Certificate.

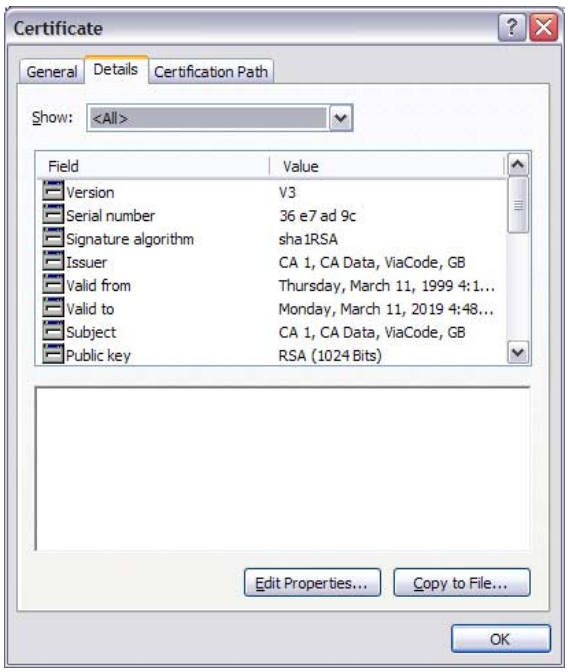


Figure 12-2 Typical Digital Certificate

The certificate contains:

- Digital Certificate Version
- Serial Number
- Signature Algorithm
- Issuer information
- Validity dates
- Subject name
- Public Key
- CRL Distribution points
- etc.

12.2.2 SELF-SIGNED CERTIFICATE

A self-signed certificate is an identity certificate that is signed by its own creator. The device software supports self-signed certificate for VPN authentication. A remote party's certificates needs to be imported as a trusted certificate.

12.3 CLI COMMANDS

This section contains typical uses of CLI Commands with PKI:

- Generating a Self-Signed Certificate on 12.3.1
- Creating a Certificate Request on 12.3.2
- Importing a certificate on 12.3.3
- Using a Certificate for a VPN tunnel on 12.3.4

For more information on CLI Commands, see the CLI Reference Guide.

12.3.1 GENERATING A SELF-SIGNED CERTIFICATE

First we need to set an identifier:

```
set pki x509 cert-fqdn support@tainet.net
```

Next, we need to generate a key pair sizes of 512, 768, 1024, 2048 supposed:

```
exec pki rsa new-key 1024
```

The following command is used to see a list of key pairs:

```
get pki x509 list key-pair
```

Next we generate a self-signed certificate:

```
exec pki x509 self-signed-cert key-pair 1
```

Once you have generated a certificate, you can see it with the following set of commands:

```
get pki x509 list cert
```

The output will be as follows:

Getting OTHER PKI OBJECT . . .

IDX	ID num	X509 Certificate Subject Distinguish Name
0	2	CN=support@tainet.net

You can also get details of the cert as follows:
get pki x509 cert 2
The output will be as follows:

```
==========================================================
X509 Certificate Details  :
Serial Number     :     02Subject :     /CN= support@tainet.net
Issuer Name       :                     /CN= support@tainet.net
==========================================================
```

12.3.2 CREATING A CERTIFICATE REQUEST

To obtain a PKCS10 certificate request based on the key pair generated:

get pki x509 pkcs10 1

The output of the command should provide the certificate request as follows:

```
----------------------BEGIN CERTIFICATE REQUEST----------------------------------
MIIBCzCBtgIBADAfMR0wGwYDVQQDFBRmd0BtaXN0bGV0b2V0ZWNoLm
NvbTBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQC+8TWjn487IZIL/PHBLjQyJ9QbSAvib
DlMptoV
2PjW9lAyx8HL7xJ5UwkRgHro8eQ77jX1BFzlXWARcFshICl3AgMBAAGgMjA
wBgkq
hkiG9w0BCQ4xIzAhMB8GA1UdEQQYMBaCFGZ3QG1pc3RsZXRvZXRlY2g
uY29tMA0G
CSqGSIb3DQEBBQUAA0EAC65SiSOOqh53bIQKpBBI8aOrhEldFL5/uzYC2
xRaN6tX
2z9O/9hiwOJoV/nugm4C+C2/UuZTWTQyLEVs53HilQ==
----------------------END CERTIFICATE REQUEST------------------------------------
```

The complete output needs to be copied and pasted on a PKCS10 based certificate enrollment webpage or provider to the CA in expected format.

12.3.3 IMPORTING A CERTIFICATE

The CA will issue a certificate based on the certificate request that we provided. This certificate can be imported into the appliance as follows:

```
exec pki x509 tftp 192.168.65.197 cert-name test.crt
```

The IP Address needs to be replaced by the IP Address of the TFTP server where the file is available and the test.crt should be replaced with the actual file name for the certificate

12.3.4 USING A CERTIFICATE FOR A VPN TUNNEL

The following commands are available to assign certificate authentication for an IKE Gateway:

```
set ike gateway test cert mycert 2 peer_cacert all peer_cert_type pkcs7
```

- The command assumes that the IKE gateway test is already created with the correct proposals.
- The mycert variable provides the cert to be used with this gateway.
- The peer_cacert all means that the peer can use a CA cert issued by any of the Cas configured on our system
- The peer_cert_type is the type of CA certificate that we are expecting the peer to send us.

Appendix A Pre-Defined Service

This appendix lists all of the pre-defined services defined on the security appliance including the name, protocol, port group, inactivity timeout and flag id. Pre-defined services use the protocol numbers listed in Table A- 1. Protocols are listed in Table A- 2.

Table A- 1 Pre-defined Service

Name	Protocol	Port Group	Timeout (min)	Flag ID
ANY	0	0/65535 other	Default	Pre-defined
AOL	6	5190/5191 remote	Default	Pre-defined
BGP	6	179 other	Default	Pre-defined
DHCP-Relay	17	67 info seeking	Default	Pre-defined
DNS	17	53 info seeking	Default	Pre-defined
FINGER	6	79 info seeking	Default	Pre-defined
FTP	6	21 remote	Default	Pre-defined
FTP-Get	6	21 remote	Default	Pre-defined
FTP-Put	6	21 remote	Default	Pre-defined
GOPHER	6	70 info seeking	Default	Pre-defined
HTTP	6	80 info seeking	Default	Pre-defined
HTTPS	6	443 security	Default	Pre-defined
ICMP-INFO	1	0/65535 other	Default	Pre-defined
ICMP-TIMESTAMP	1	0/65535 other	Default	Pre-defined
IKE	17	500 security	Default	Pre-defined
Internet Locator Service	6	389 info seeking	Default	Pre-defined
IRC	6	6660/6669 remote	Default	Pre-defined
L2TP	6	1701 remote	Default	Pre-defined
LDAP	6	389 info seeking	Default	Pre-defined
MAIL	6	25 email	Default	Pre-defined
NetMeeting	6	1720 remote	Default	Pre-defined

Name	Protocol	Port Group	Timeout (min)	Flag ID
NFS	17	111 reChapter 1mote	Default	Pre-defined
NNTP	6	119 info seeking	Default	Pre-defined
NTP	17	123 other	Default	Pre-defined
PC-Anywhere	17	5632 remote	Default	Pre-defined
PING	1	0/65535 other	Default	Pre-defined
POP3	6	110 email	Default	Pre-defined
PPTP	6	1723 security	Defautl	Pre-defined
Real Media	6	7070 info seeking	Default	Pre-defined
RLOGIN	6	513 remote	Default	Pre-defined
SNMP	17	161 other	Default	Pre-defined
SSH	6	22 security	Default	Pre-defined
SYSLOG	17	514 other	Default	Pre-defined
TALK	17	517/518 other	Default	Pre-defined
TCP-ANY	6	0/65535 other	Default	Pre-defined
TELNET	6	23 remote	Default	Pre-defined
TFTP	17	69 remote	Default	Pre-defined
TRACEROUTE	1	0/65535 other	Default	Pre-defined
UDP-ANY	17	0/65535 other	Default	Pre-defined
UUCP	17	540 remote	Default	Pre-defined
VDO Live	6	7000/7010 info seeking	Default	Pre-defined
WINFRAME	6	1494 remote	Default	Pre-defined
X-WINDOWS	6	6000/6063 remote	Default	Pre-defined

Table A- 2 Protocols

Protocol	Protocol Number
TCP	6
UDP	17
ICMP	1

Appendix B Glossary

1000Base-T: The specification that describes the use of Gigabit Ethernet over copper Cat-5 wire. It defines data rates of 1 Gigabit per second Gb/s over a distance not to exceed 100 meters.

Advanced Encryption Standard (AES): An emerging encryption standard that can use a 128-, 192-, or 256-bit encryption key. This new standard supports easier interoperability with other security appliances as it becomes widely adapted.

Address Resolution Protocol (ARP): A protocol used to map an internal IP address to physical machines that a local network recognizes. A table called an ARP Cache stores and correlates the IP address and physical address assigned for a specific host. ARP provides the protocol rules for making this correlation and provides address communication in both directions.

Advertisement: A method used by routers to send information to other network devices. This could include an IP address, network mask or other data.

Authentication Header (AH): A method that provides integrity and authentication, but not privacy, as IP data is not encrypted. AH contains an authentication value based on a symmetric-key hash function.

Bridge: A device that enables the connection of multiple network segments while using the same network and mask.

Data Encryption Standard (DES): A standard that uses either a 40 or 56 bit encryption algorithm developed by the National Institute of Standards and Technology (NIST). DES uses a block encryption method that was originally developed by IBM in the 1970s. The U. S. Government has since certified it to transmit data that has not been as classified “top secret.” DES uses a 64-bit key to encrypt and decrypt data into 64-bit block enabling it fixed output for variable

length input.

Data Encryption Standard-Cipher Block Chaining (DES-CBC):

Standard that enables the use of Triple DES (or 3DES). By enabling CBC, the DES encryption occurs three times, enabling generation of the 56-bit key three times. The 3DES standard uses a key length of 168-bits.

Datagram: A self contained data packet sent over an IP network.

Default Route: A standard entry in a routing table that enables traffic to be forwarded for destination networks that are not explicitly defined on a specific network device. The normal representation of the default route is 0.0.0.0/0.

Demilitarized Zone (DMZ): Usually a small network that sits between the trusted local area network (LAN) and the public Internet. DMZ enables administrators to apply different polices to traffic that might need to be accessed from the public Internet.

Domain Name: A name that can identify one or more IP addresses. URLs normally use domain names to identify particular web pages.

Domain Name System (DNS): An Internet system that translates domain names into IP addresses.

Dynamic host configuration protocol (DHCP): Protocol that automatically assigns IP addresses to computers on a local area network (LAN). Typically, a system administrator designates a range of IP addresses that DHCP assigns. Each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server. This protocol reduces the work necessary to administer a large IP network.

Encryption: The ability for a network device to translate data into a secret code. Encryption is an effective way to protect data so that only the intended recipient can decode it. All encryption uses a public/private key pairing so that a user can encrypt and decrypt the specific data. A device allows encryption using the private key, and only users with the public key can decrypt that information.

Encapsulating Security Payload (ESP/AH): Protocol that defines the IP security

used for the protocol, IP Security (IPsec). IPsec defines the keys, algorithms and networks that are encrypted. ESP provides both authentication and encryption, while AH or Authentication provides only authentication. ESP is defined as protocol 50.

Ethernet: A local area network (LAN) technology developed by Xerox Corporation along with DEC and Intel in the 1970s. Ethernet is a best-effort technology that uses Carrier Sense Multiple Access/ Collision Detection (CSMA/CD) technology. Ethernet is flexible and can run over a variety of cables including coaxial, thin coaxial, twisted pair and fiber optic. Ethernet defines the standard for which computers connect in a LAN segment.

Extended Authentication (XAUTH): A method to perform user authentication in a separate phase after the IKE authentication or phase 1 exchange. The authentication name must match the XAUTH configuration name in order to allow the user to authentication and permit access.

Firewall: A hardware device or software application (or a combination of both) that provides a system that protects a network segment from unauthorized use, usually from Internet “hackers.” Most firewalls are installed to protect users from unauthorized Internet access, but can be deployed to create additional network security.

File Transfer Protocol (FTP): A protocol used to transfer data over a network or the Internet. FTP is commonly used to download or upload files from or to a server.

Gateway: A special-purpose device often referred to as a router that transfers IP datagrams from one network to another until they reach their final destination.

High Availability (HA): Provides the ability to service end users (i.e., sessions) with little or no interruption when failures occur.

Host Name: A unique name that a host on a network is known as and is used to identify the host during data transfers.

Hyper Text Transfer Protocol (HTTP): The protocol that the World Wide Web uses. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

Hub: A common connection point for multiple devices on a local area network (LAN) segment. As traffic is sent to a hub port, the hub port forwards it to all other ports on the hub so all other network devices can view that traffic.

Internet Control Message Protocol (ICMP): An extension of IP used to report packet errors and control or transmit information. Ping is an example of an ICMP message that is used to test connectivity of a device.

Internet: A network that allows millions of computers to be connected as a single global network. Originally developed by the U. S. Defense Department, the Internet was designed as a way to prevent communication breakdown in the event of nuclear war. Today the Internet is used as a way to share information including e-mail, files, and newsgroups.

Internet Key Exchange (IKE): A method used to exchange keys to encrypt and authenticate data over an unsecured medium, such as the Internet.

Internet Protocol (IP): Protocol that specifies the format for a packet, also called a datagram. Datagrams are commonly used in connectionless, best-effort delivery systems like the Internet. IP defines how information is passed between systems across a network.

IP Address: A32-bit numeric address with four spaces, usually separated by a period, that identifies a node or network device. An IP address can be a combination of four numbers from 0 through 255. For example, 172.16.31.2 represents an IP address.

IP Security (IPsec): A set of protocols developed by the Internet Engineering Task Force (IETF) to enable secure exchange at the IP level. The most common implementation of IPsec is seen in virtual private network (VPN) deployments. IPsec enables VPNs to take advantage of authentication, integrity, and confidentiality.

Internet Security Association and Key Management Protocol (ISAKMP): Protocol that uses a common framework to provide information about Security Association (SA) attributes. These include the negotiation, modification, and deletion of SA.

Local Area Network (LAN): Any network technology that connects multiple

machines in a local office or building. LAN networks usually consist of a main connection point like a switch or hub and enable all machines on that segment to communicate. LAN networks have a limited range of around 1,640 feet or 500 meters.

Man in the Middle Attack (MTM): Incident allowing a “hacker” to read, insert, and modify all messages between two parties without the parties knowing their link was compromised. The attacker must have the ability to observe and intercept all messages going between the two victims.

Maximum Transmission Unit (MTU): The largest physical packet size, measure in bytes that a network can transmit. Any messages larger than the MTU divide into smaller packets before being sent.

Message Digest 5 (MD5): A one-way hash function. This hash function takes a variable length message and formats it to a fixed length using a 16-bit key to produce 128-bit hash.

Media Access Control (MAC) Address: The hardware address that uniquely defines each Ethernet interface in use on a local area network (LAN). The MAC address commonly refers to the Ethernet address or a node on a LAN. When connected to the Internet, the MAC address tracks the IP address of a node. The <NetSecure 6100> software creates a table that references the MAC address to a known IP address.

NAT-Traversal (NAT-T): Network Address Translation method that allows IP Security (IPsec) packets to pass through a NAT device that might be along its path by detecting and encapsulating the Internet Key Exchange (IKE) packets as User Datagram Protocol (UDP). The most common port used to perform NAT-T is UDP port 500.

Netmask: Identifies the sub-network and the hosts that are available. An example, 10.0.0.0 255.255.255.0 (10.0.0.0/24) refers to all hosts in the 10.0.0.0 subnet.

Network Address Translation (NAT): A standard that allows machines on a local area network (LAN) to use a set of IP addresses for internal use and another IP address or set of addresses to access external traffic. Most NAT devices are used to enable multiple machines on a LAN to access the Internet using a single external address.

Network Time Protocol (NTP): Protocol built on top of TCP/IP and used to synchronize local timekeeping with reference to radio, atomic, or other clocks located on the Internet. This protocol is capable of providing accuracies typically within a millisecond to a network device.

Next Hop: An IP address used in a routing table to enable forwarding of traffic for a specific network.

Packet: A unit of data routed between a source and destination over the Internet or a packet-switched network.

Public Key Infrastructure (PKI): PKI is designed to be used with IPSec instead of PSK and Manual Key. It provides a higher level of security.

Port Address Translation (PAT): Translates the original source port number to a different, randomly assigned port number.

Port Mapping: Changes the original destination port number on a packet to a different, predetermined port number.

PPPoE: Point-to-Point Protocol over Ethernet. Used to allow ISPs the use of their existing Radius authentication systems from their Dial-Up service on a Broadband/Ethernet-based service.

Remote authentication dial-in user service (RADIUS): provides an authentication, authorization and accounting protocol for applications such as network access or IP mobility. When used it is intended to work in both local and remote situations.

RJ-45: An 8-wire connector commonly used to connect multiple computers into a local area network (LAN). Standard RJ-45 connectors are slightly wider than the standard RJ-11 connector used for all telephone connections.

Router: A device that forwards packets between various networks using both the network layer information and router tables. Routers can be used either on a local area network (LAN) or wide area network (WAN). The most command use for a router is to connect a LAN to an Internet Service Provider (ISP).

Routing Information Protocol (RIP): One of the most commonly used interior

gateway protocol (IGP) routing protocols on internal networks (and to a lesser extent, networks connected to the Internet), which helps routers dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are.

Routing Table: Table that contains real-time information on all networks available through the router. Most routing tables include media access control (MAC) and IP address information.

Secure Hash Algorithm-1 (SHA-1): A one-way hash function. This hash function takes variable length messages and formats it to a fixed length using a 20-byte key to produce a 160-bit hash.

Secure Shell (SSH): A protocol that enables secure device management. SSH is used to securely manage the <NetSecure 6100>.

Security Association (SA): A method for creating a virtual private network (VPN) tunnel. The SA includes all of the required security perimeters to secure communication. Since this communication is bidirectional, two SAs are required to establish communication.

Security Parameter Index (SPI): A hexadecimal number used to uniquely define each virtual private network (VPN) tunnel. The SPI determines which key the <NetSecure 6100> uses to encrypt or decrypt packets.

Simple Network Management Protocol (SNMP): forms part of the internet protocol suite as defined by the Internet Engineering Task Force. The protocol is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention.

Static Route: A user-definable route that defines how a packet is to move between a source and destination. Static routes are a manual entry that allows administrators to set default-route mapping before the beginning of a route. These routes work well in networks that have a predictable path for all network traffic.

Subinterface: A logical segment for a physical connection. A subinterface allows administrators to split the bandwidth between multiple networks connected to the same physical port. On the <NetSecure 6100>, the IEEE standard 802.1Q is used to tag and identify the subinterface.

Subnet: A network that shares a common address component. Subnets are defined as all hosts whose IP addresses have the same prefix on a TCP/IP network.

Subnet Mask: Determines the subnet an IP address belongs to. The subnet mask also enables networks to be broken into smaller blocks.

Syslog: A protocol used to generate and send log messages. Syslog traffic is usually sent to a host running a syslog daemon allowing collection and storage of log messages from a network device.

Transmission Control Protocol/Internet Protocol (TCP/IP): A set of communication protocols that defines how a host communicates with another host. Hosts can be located on the same local area network (LAN) or across a wide area network (WAN). TCP/IP allows machines to communicate even if they do not use the same operating system.

Trivial File Transfer Protocol (TFTP): A simple form of the File Transfer Protocol (FTP) that uses User Datagram Protocol (UDP) to transfer data and provides no security.

User Datagram Protocol (UDP): A connectionless protocol that, like TCP, runs within an IP network. UDP runs fewer error checks and is classified as a best-effort protocol.

Uniform Resource Locator (URL): The standard used to obtain the location of resources or global addresses found on the World Wide Web.

Unshielded Twisted Pair (UTP): A standard cable used for telephone lines, UTP is also used for Ethernet connections and is often referred to as 10BaseT.

Virtual Local Area Network (VLAN): A logical collection of nodes on a network rather than a physical collection. It enables the nodes to be in the same broadcast domain even though they might not be located on the same physical switch. Users on the VLAN are identified using tags in the frame header and are often referred to in the IEEE standard 802.1Q.

Virtual Private Networking (VPN): An easy, cost-effective way for business to use the public Internet to allow secure remote access into a private network.

VPNs commonly use encryption and authentication to make this communication secure.

Wide Area Network (WAN: A computer network that spans a large geographical area. Typically a WAN consists of two or more local area networks (LAN), usually connected using the public telephone system, leased lines or satellite. The largest WAN today is the Internet.

Zone: A segment on a network where certain security parameters are applied. This could include a security zone, virtual private network (VPN) zone, or demilitarized zone.